Public Document Pack

Economic Security and Cyber Crime Committee

Date: **TUESDAY, 23 JUNE 2026**

Time: 11.00 am

Venue: **COMMITTEE ROOMS, 2ND FLOOR, WEST WING, GUILDHALL**

Members:

Tijs Broeke (Chair)
Deputy Madush Gupta
Melissa Collett
Jason Groves
Naresh Hari Sonpar
Mandeep Thandi
Deputy James Thomson CBE
James Tumbridge
Deputy Dawn Wright
Kwaku Osafo
Michael Landau
Philip Kelvin
Andrew Lentin

Enquiries: **Kezia Barrass**
Kezia.Barrass@cityoflondon.gov.uk

Accessing the virtual public meeting

Members of the public can observe all virtual public meetings of the City of London Corporation by following the below link:
https://www.youtube.com/@CityofLondonCorporation/streams

A recording of the public meeting will be available via the above link following the end of the public meeting for up to one civic year. Please note: Online meeting recordings do not constitute the formal minutes of the meeting; minutes are written and are available on the City of London Corporation's website. Recordings may be edited, at the discretion of the proper officer, to remove any inappropriate material.

Whilst we endeavour to livestream all of our public meetings, this is not always possible due to technical difficulties. In these instances, if possible, a recording will be uploaded following the end of the meeting.

Ian Thomas CBE
Town Clerk and Chief Executive

AGENDA

Part 1 - Public Agenda

1. **APOLOGIES**

2. **MEMBER'S DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**

3. **ELECTION OF DEPUTY CHAIR**

   To elect a Deputy Chair in accordance with standing Order 29

   For Decision

4. **MINUTES**

   To approve the public minutes and non-public summary of the meeting held on 23 February 2026

   For Decision
   (Pages 5 - 8)

5. **DEPUTY COMMISSIONER'S UPDATE**

   Report of the Commissioner

   For Information
   (Pages 9 - 12)

6. **POLICING PLAN PERFORMANCE REPORT Q4 2025/26**

   Report of the Commissioner

   For Information
   (Pages 13 - 58)

7. **SUMMARY OF ACTION FRAUD PUBLIC COMPLAINTS DATA - Q4 2025/26**

   Report of the Commissioner

   For Information
   (Pages 59 - 64)

8. **INNOVATION & GROWTH - UPDATE ON ECONOMIC SECURITY AND CYBER CRIME RELATED ACTIVITIES**

   Report of the Executive director, Innovation and Growth

For Information
(Pages 65 - 70)

9. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**

10. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**

11. **EXCLUSION OF THE PUBLIC**

MOTION - That under Section 100(A) of the Local Government Act 1972, the public be excluded from the meeting for the following item(s) on the grounds that they involve the likely disclosure of exempt information as defined in Part I of Schedule 12A of the Local Government Act.

For Decision

Part 2 - Non-Public Agenda

12. **NON-PUBLIC MINUTES**

To agree the non-public minutes of the meeting held on 23 February 2026

For Decision
(Pages 71 - 74)

13. **FCCRAS PROGRAMME CLOSURE & LESSONS LEARNED**

Report of the Commissioner

For Information
(Pages 75 - 178)

14. **STRATEGIC COMMUNICATIONS AND ENGAGEMENT PLAN FOR ECONOMIC AND CYBER CRIME**

Report of the Town Clerk and the Commissioner

For Information
(Pages 179 - 190)

15. **PALANTIR'S ROLE IN THE REPORT FRAUD SERVICE**

Report of the Commissioner

For Information
(Pages 191 - 200)

16. **DOMESTIC CORRUPTION UNIT - ASSESSING BENEFITS AND PERFORMANCE**

Report of the Commissioner

For Information
(Pages 201 - 208)

17. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**

18. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**

ECONOMIC SECURITY AND CYBER CRIME COMMITTEE
Monday, 23 February 2026

Minutes of the meeting of the Economic Security and Cyber Crime Committee held at Committee Rooms, 2nd Floor, West Wing, Guildhall on Monday, 23 February 2026 at 11.00 am

Present

Members:

Tijs Broeke (Chair)
Deputy Madush Gupta (Deputy Chair)
Melissa Collett
Naresh Hari Sonpar
Mandeep Thandi
Deputy James Thomson CBE
Kwaku Osafo

Officers

Richard Riley CBE	-	Town Clerk's Department
Oliver Bolton	-	Town Clerk's Department
Preet Desai	-	Town Clerk's Department
Kezia Barrass	-	Town Clerk's Department
Mary Kyle	-	Innovation and Growth

City of London Police:

Nik Adams	-	City of London Police
Ollie Shaw,	-	City of London Police
Lucy Cumming,	-	City of London Police
Emma Cunnington,	-	City of London Police
Andrew Gould, Blair Stringman,	-	City of London Police
Glenn Sebright,	-	City of London Police
Matthew Bradford,	-	City of London Police
Nicola Atter,	-	City of London Police
Phoebe Murphy,	-	City of London Police
Thomas Hill,	-	City of London Police
Douglas Ing,	-	City of London Police
Patrick Milford,	-	City of London Police

1. **APOLOGIES**
   Apologies were received from Dawn Wright and James Tumbridge

2. **MEMBER'S DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**
   There were no declarations.

3. **MINUTES**

RESOLVED, - that the public minutes and non-public summary of the meeting held on 4 November be approved as an accurate record, subject to the amendments made to the officers in attendance and the note of apologies from James Tumbridge.

4. **PUBLIC OUTSTANDING ACTIONS**

Members received a report of the Commissioner which outlined outstanding actions.
RESOLVED, - that the report be noted.

5. **DEPUTY COMMISSIONER'S UPDATE (NATIONAL LEADERSHIP FUNCTIONS)**

Members received a report of the Commissioner which provided an update on the national leadership functions.
RESOLVED, - that the Deputy Commissioner was heard.

6. **POLICING PLAN PERFORMANCE REPORT - Q3 2025/26**

Members received a report of the Commissioner which outlined the Policing Plan performance report from Q3 of 2025/26.
Members noted ongoing collaboration with HMICFRS to support the learning taken from the previous inspection, and to allow improved delivery against the recommendations and findings in the City. Officers were working with Tower Hamlets to ensure a proactive approach to tackling Fraud, and assured Members of their confidence that the internal governance in place would put City of London Police in a strong position for future inspections.
Members discussed the use of social media and encouraged officers to consider how to shift from transactional information sharing to more targeted and dynamic campaigns.
RESOLVED, - that the report be noted.

7. **NLF PERFORMANCE FRAMEWORK REFRESH**

Members received a report of the Commissioner which provided an update on the National Lead Force performance framework refresh.
Members welcomed the report and were pleased to see the ambitious targets set, but requested more specific figures which would show the goals as a percentage increase of the current figure. Officers assured Members that detailed breakdowns would accompany future reports and that this would be a useful tool to evidence the impact of ongoing work.
RESOLVED, - that the report be noted.

8. **SUMMARY OF ACTION FRAUD PUBLIC COMPLAINTS DATA**

Members received a report of the Commissioner which summarised Action Fraud public complaints data.
RESOLVED, - that the report be noted.

9. **CYBER RESILIENCE CENTRE (CRC) NETWORK UPDATE**

Members received a report of the Commissioner which provided an update on the Cyber Resilience Centre Network.

Members congratulated officers on the launch of the CRC Network and the success of the summit and noted it had been a difficult transition which took longer than initially anticipated. Members discussed the opportunities to build on and support this work in future. The Police Authority team agreed to review the structure of the NCRCG and the governance structure of the Cyber Resilience Board.
RESOLVED, - that the report be noted.

10. **INNOVATION & GROWTH - UPDATE OF CYBER & ECONOMIC CRIME RELATED ACTIVITIES**
Members received a report of the Executive Director of Innovation & Growth which provided updates on cyber and economic crime related activities.
Members welcomed the report and discussed the threat and opportunities related to AI and quantum computing. Officers shared that there was no specific activity on this planned, but they expected to have an update to share with Members at the next ESCCC meeting. Members expressed the need for urgent organisational readiness given the risk posed to data encryption and long-term security.
Members noted that City of London Police were developing AI agents on the Report Fraud to augment the capacity as National Lead Force and would provide a report on this at a future committee meeting.
RESOLVED, - that the report be noted.

11. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
There were no questions.

12. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**
There was no other business.

13. **EXCLUSION OF THE PUBLIC**
RESOLVED, - That under Section 100(A) of the Local Government Act 1972, the public be excluded from the meeting for the following item(s) on the grounds that they involve the likely disclosure of exempt information as defined in Part I of Schedule 12A of the Local Government Act.

14. **NON-PUBLIC MINUTES**
RESOLVED, - that the non-public minutes of the meeting held on 4 November 2025 were approved as an accurate record.

15. **NON-PUBLIC OUTSTANDING ACTIONS**
Members received a joint report of the Town Clerk and the Commissioner which outlined non-public outstanding actions.

16. **DOMESTIC CORRUPTION UNIT 2026-2029**
Members received a report of the Commissioner which sought endorsement for the City of London Police to proceed with the implementation phase of the Domestic

17. **FCCRAS UPDATE**
Members received a report of the Commissioner which provided an update on the Fraud and Cyber Crime Reporting and Analysis Service.

18. **REPORT FRAUD FULL LAUNCH PRESENTATION**

Members received a report of the Commissioner which provided the Report Fraud full launch presentation.

At 12:58 the meeting was extended under Standing Order 39

19. **CITY OF LONDON POLICE ASSET MANAGEMENT OFFICE**
Members received a report of the Commissioner which covered the City of London Police Asset Management office.

20. **STRATEGIC COMMUNICATIONS AND ENGAGEMENT PLAN FOR ECONOMIC AND CYBER CRIME**
Members received a report of the Town Clerk which outlined the strategic communications and engagement plan for economic and cyber crime.

21. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
There were no questions.

22. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**
There was one item of non-public business.

The meeting ended at 13:04

Chairman

Contact Officer: Kezia Barrass
Kezia.Barrass@**cityoflondon.gov.uk**

City of London Corporation Committee Report

Committee(s): Economic Security & Cyber Crime Committee – For Information	**Dated:** 23/06/2026
Subject: Deputy Commissioner's Update	**Public report:** For Information
This proposal: **1. delivers Corporate Plan 2024-29 outcomes**	Dynamic Economic Growth, Providing Excellent Services
Does this proposal require extra revenue and/or capital spending?	No
If so, how much?	£0
What is the source of Funding?	N/A
Has this Funding Source been agreed with the Chamberlain's Department?	N/A
Report of:	Deputy Commissioner Nik Adams
Report author:	DI Anna Martin

Summary

This report provides an update from the Deputy Commissioner of NLF activity since the last meeting of the Economic Security and Cyber Crime Committee.

Recommendation

Members are asked to note the report.

Main Report

1. The following report outlines notable activity in the last quarter delivered by National Functions (City of London Police).

Strategic Leadership and Engagement

2. March saw the launch of the much awaited Fraud Strategy with Commissioner O'Doherty and Commander Shaw attending the launch event led by the Rt Hon. Lord Hanson. The CoLP Economic and Cyber Crime Policing HQ team

have commenced work to rewrite the national policing strategy for fraud, economic and cyber crime to align with the new government strategy.

3. Throughout the last quarter, significant time and focus has been devoted to preparing the CoLP submission documents in response to the government's announcement on Police Reform. This includes a draft proposal for the future of CoLP's national functions in relation to fraud. Strategic engagement activity also remains a priority as we seek to garner support from industry partners who benefit from the unique capabilities that CoLP deliver.

4. In March the Commissioner, Deputy Commissioner and other senior CoLP staff attended the Global Fraud Summit in Vienna in March, hosted by Interpol and the United Nations Office on Drugs and Crime. A significant proportion of the planning was delivered by DSU Nick Court, the CoLP secondee into Interpol. This high-level event brought together ministers and senior representatives from across governments, law enforcement, private sector, civil society organizations and international organizations. Commissioner O'Doherty, and other senior leaders participated inpanel sessions and bilaterals which was well received.

5. The NPCC Money Laundering and Asset Recovery portfolio continues to strengthen and deliver new capabilities. Recent developments include: developing proposals in response to an increase in the Economic Crime Levy, preparation for the forthcoming Financial Action Task Force (FATF) inspection in August 2027, continued implementation of a UK Asset Management Office and leading the transformation of the Joint Asset Recovery Database via the ARIT Programme.

6. May saw the announcement of the Home Office's High Street Organised Crime Unit, a new task force focussed on cash-based money laundering and cross cutting organised criminality which is impacting on our High Streets. Commander Ollie Shaw attended a Ministerial Round Table to shape this work in line with the work previously delivered by the economic crime portfolio on Operation Machinize.

7. Our latest cohort of Police Now Direct Entry Economic and Cyber Crime detectives are currently undergoing their initial training, with several forces now signed up to and supporting the scheme. In June, CoLP will be welcoming the Rt Hon. Lord Hanson to GYE where he will learn more about the pathway and the positive impact it is having on our fraud, economic and cyber crime response nationally. Our Accredited Economic Crime Professional pathway programme has received ministerial sign off and will continue to be owned and developed by CoLP with short to medium funding fully secured.

8. The Fraud and Cyber First Responder training package has been delivered as a joint programme with the College of Policing and the Economic and Cyber Crime Academy. This online training provision, provides officer and staff first responders with a baseline knowledge of what fraud and cyber crime is, how

to respond and advise victims an overview of the Report Fraud system. Media and comms will launch this from the end of June.

Operational Highlights

9. Operation Henhouse 5 took place in February 2026 and was the most successful iteration yet of this annual intensification. Coordinated by the Lead Force Operations Room (CoLP) and the National Economic and Crime Centre (NCA), this national operation involved a month long period of coordinated activity against fraud offenders across the country, involving all Home Office police forces along with other law enforcement agencies. Results included 557 arrests, 249 cease and desist notices issued, 172 voluntary interviews, £9 million secured through Account Freezing Orders, £2.8 million in cash seizures and £15.3 million in non-cash asset seizures.

   City of London Police teams also supported Operation Henhouse operational activity. The Fraud Operations team executed a search warrant and arrest of a fraud offender in South London where they were accompanied by the Rt Hon. Lord Hanson MP.

10. Officers from the Police Intellectual Property Crime Unit (PIPCU) made eight arrests, executed 19 search warrants and carried out seven cease and desist actions. They also secured 15 account freezing orders, totalling £537,000. In addition, officers seized more than 7,000 counterfeit items, representing an estimated £700,000 loss to industry.

11. The Insurance Fraud Enforcement Department (IFED) made 11 arrests and issued 63 cease and desist orders. Five of the arrests formed part of an operation targeting ‘ghost broking’, including the arrest of a former Metropolitan Police officer. The investigation uncovered thousands of fake insurance certificates and a network selling spoof apps designed to deceive officers during roadside checks. The unit also seized £5,000 in cash and £20,000 worth of Rolex watches.

12. The Dedicated Card and Payment Crime Unit (DCPCU) carried out 31 arrests and interviews under caution and seizing more than £48,000 in cash and non-cash assets. Officers also recovered fake ID printing equipment and SMS blaster devices, each valued at approximately £10,000, preventing their further use in criminal activity. In addition, the unit secured two account freezing orders totalling £589,000 linked to money laundering. During the operation the Head of Fraud Prevention and Training at DCPCU delivered fraud prevention training to bank staff and customers across multiple branches. In total, 13 sessions were delivered to more than 800 people, reinforcing the unit’s commitment to protecting the public from financial crime.

13. Two offenders have been sentenced at Southwark Crown Court following a DCPCU investigation Operation Triton. Between June 2020 and November 2022, the offenders provided a ‘smishing service’ where they would issue mass fraudulent text messages on behalf of other criminals. These messages

would often impersonate genuine organisations such as banks and government departments and aimed to trick the receiver into clicking on a link and in putting personal details which included names, birthdays, bank details and further security information. Following a complex investigation, DCPCU were able to obtain evidence of large-scale offending from details found on the mobile phones of both offenders. On 30th April 2026 they were sentenced to 27 months imprisonment and 8 months imprisonment (suspended for 12 months) & 120 hours unpaid work for their involvement.

Media Highlights

14. Positive media coverage in several mainstream and LGBTQ+ outlets followed the sentencing of a male who defrauded three gay male victims out of nearly £30K using dating apps. This investigation, led by our Fraud Operations team, saw the offender sentenced to three years imprisonment after he targeted his victims online, pretending to be gay man seeking a long term relationship, and persuaded them to send him sums of money in the belief that they were in a relationship.

15. BBC North West reported on a series of warrants executed in Oldham by our PIPCU team, supported by the North West ROCU, also attended by representatives from the Intellectual Property Office. Several shipping containers were located containing imitation designer clothes, shoes, bags and cosmetics.

Anna Martin
Detective Inspector (Staff Officer)

T: 07720 103030
E: anna.martin@cityoflondon.police.uk

City of London Corporation Committee Report

Committee(s): Economic Security and Cyber Crime Committee	**Dated:** 23 June 2026
Subject: Policing Plan Performance Report Q4 2025/26	**Public report:** For Information
This proposal: • **delivers Corporate Plan 2024-29 outcomes** • **provides statutory duties**	Diverse Engaged Communities, Dynamic Economic Growth, Vibrant Thriving Destination, Providing Excellent Services
Does this proposal require extra revenue and/or capital spending?	No
If so, how much?	£-
What is the source of Funding?	N/A
Has this Funding Source been agreed with the Chamberlain's Department?	N/A
Report of:	Commissioner of City of London Police
Report author:	T/Ch Insp Megan Cardy, Head of Force Performance

Summary

The appendices of this report summarises the Policing Plan Performance for Q4 in 2025/26.

Appendix 1 outlines the National Delivery Plan Performance Report for Q4 2025/26, which assesses the national policing performance against the objectives set out in the National Policing Strategy for Fraud, Economic and Cyber Crime 2023-28.

Appendix 2 provides an assessment of City of London Police performance against the objectives set out in the National Policing Strategy for Fraud, Economic and Cyber Crime (2023-28).

Appendix 3 provides an example of the product that will be presented to Members to show performance for fraud in 2026/27.

Recommendation

Members are asked to:

- Note the report and appendices.

Appendices

- Appendix 1: National Delivery Plan Performance Report Q4 2025/26
- Appendix 2: City of London Police (NLF) Performance Report Q4 2025/26

- Appendix 3: Policing Plan Performance Fraud Slides Example

T/Ch Insp Megan Cardy
Head of Force Performance

National Lead Force
National Delivery Plan Performance Report

FY 2025/26
Q4: January – February 2026

Performance Assessment

The dashboard provides an assessment of national policing performance against the objectives set out in the **National Policing Strategy for Fraud, Economic and Cyber Crime 2023-28**. The National Policing Strategy was launched in November 2023 and translates national strategies and objectives set by His Majesties Government into actionable measures for policing in the areas of fraud, money laundering and asset recovery and cyber. The report shows national attainment against the objectives. The National Policing Strategy sets out a purpose to "improve the UK policing response to fraud, economic and cyber crime" through three **key cross cutting objectives** of: Improving outcomes for victims; Proactively pursuing offenders; Protecting people and business from the threat

The NLF plan seeks out **key cross cutting enabling commitments** that City of London Police is seeking to achieve		**FYTD Performance**	**Data Trend**
Money Laundering Asset Recovery 1	We will increase disruptions against money laundering offenders.		⇩
Money Laundering Asset Recovery 2	We will seize and restrain more criminal assets through including released asset denial activity		⇩
Money Laundering Asset Recovery 3	We will provide training to policing on how to investigate and seize crypto assets. We will ensure accurate records of crypto assets seizures are maintained and provided.		
Fraud 1	We will increase the policing response and outcomes linked to National Fraud Intelligence Bureau/ Fraud and Cyber Crime Reporting Analysis System crime dissemination packages.		⇨
Fraud 2	We will deliver and co-ordinate regional Proactive Economic Crime Teams and uplifted National Lead Force teams to form part of the National Fraud Squad. The National Fraud Squad teams will proactively target fraudsters and disrupt offending achieving criminal justice and alternative outcomes.		⇩
Fraud 3	We will lead the National Fraud Squad to PURSUE identified high harm offenders through joint, centrally co-ordinated national operations and to participate in National Economic Crime Centre led fraud intensifications throughout the year.		⇧
Fraud 4	We will support and assist the national development and implementation of the Fraud Targeting Cell by contributing resource and supporting the delivery of systems and processes. We will increase intelligence packages into the system leading to increased proactive operations.		⇧
Fraud 5	We will develop and deliver a centrally co-ordinated National Fraud PROTECT Network that will align with the National Cyber PROTECT Network, share best practice, and promote local delivery of national messaging.		⇩

Performance Assessment

		FYTD Performance	Data Trend
Cyber 1	We will increase the policing response and outcomes linked to NFIB / Report Fraud crime dissemination packages. We will ensure full and timely compliance from forces to record disseminations from the NFIB appropriately and that subsequent outcomes are reported back to NFIB correctly.		⇩
Cyber 2	We will increase intelligence led proactive operations and self-development operations regarding Computer Misuse Act offending, ensuring the relevant deconfliction safeguards are followed.		⇩
Cyber 3	We will develop the current PROTECT notification processes to ensure a consistent approach to both the direct PROTECT officer taskings and the notifications delivered at scale.		⇨
Cyber 4	We will ensure ROCUs and Forces are regularly using Police Cyber Alarm to help support member organisations when issues are identified and use the data to inform and drive PROTECT, PREVENT and PURSUE activity. PROTECT Officers will promote Police Cyber Alarm to all SME organisations they engage with.		⇩
Cyber 5	We will deliver the new NPCC Cyber Resilience Centre (CRC) Model. This includes the new Operating Model to deliver the levels of consistency and assurance required. CRCs and PROTECT officers will work together to support each other's work and grow CRC membership.		⇩
Cyber 6	We will develop improved referral process for new nominals to include Target Operating Model and definition of when a referral should be made. We will introduce a single national or regional referral mechanism and implement risk assessment (CORA) and tasking mechanisms for PREVENT referrals.		⇨
Cyber 7	We will roll out the Cyber & Digital Specials & Volunteers (CDSV) Programme and platform to every region and Force and ensure effective management and utilisation of CDSV skills across the network.		⇩
Cyber 8	We will revise and roll out a clear training, CPD and accreditation pathway for all roles within TCUK, with regular reviews of the training needs analysis and advancements in technology / threats. NPCC Deliver new strategy and delivery with the Economic and Cybercrime Academy.		⇩

Executive Summary

It is not possible to report an outcome picture for Q3 and Q4 as changed to processes since Report Fraud's introduction mean like for like data is not currently available.

However the volume of crime reports sent for investigation to forces has increased significantly in Q4 a large proportion of this is "call for service" disseminations where an investigation is already under way locally being sent to police forces confirming their investigative force status.

A significant increase in Cyber training delegates was seen in Q4 however due to the challenges with funding and service provider contracts earlier in the year (FQ1 and FQ2) the service level set for the year has not been met.

A decrease in disruptions was seen in Q4 and year on year for both Cyber and Economic Crime areas of SOC disruption, with decreases seen in Q4 for fraud also. This reduction is in part due to a realignment of recording practices and their implementation by the NCA that have impacted SOC disruptions across all sectors nationally.

It is also acknowledged that the Joint Asset Recovery Data set is a more effective data set for Asset seizures and will be used in future reporting practices as aligned to the Home Office reporting for this area.

Police Cyber alarm and Cyber Resilience Centre sign ups were significantly reduced in Q3 and Q4 and therefore have not met the service level for this financial year.These reductions are seen as we transitioned to a new structure for the Cyber Resilience Centre's and procured a new supplier for Police Cyber Alarm.

It is expected that improvements in this area will be seen under the new structure and performance reporting is in place to monitor this.

Overall protect engagements have reduced in the financial year with the change to the way protect was managed and the onboarding of the new Report Fraud system being a focus.

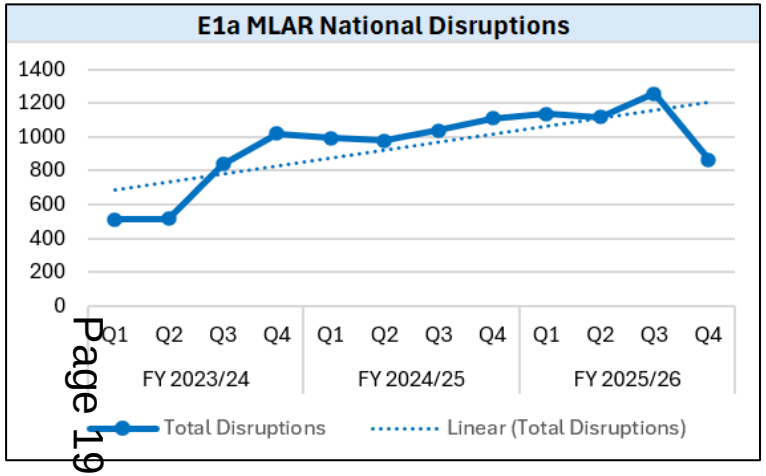
The satisfaction with protect engagement remains high and COLP is looking to understand further how it understands the impact from engagement events as well as the satisfaction.

Money Laundering and Asset Recovery

Improve Outcomes for Victims

Performance Measure 1: We will increase disruptions against money laundering offenders.

Success Measures:	FYTD Performance	Data Trend
E1a Increase the number of recorded disruptions linked to money laundering and or illicit finance – **Home Office Measure**		⇩



Op Falcon

For Q4, the largest operation resulting in 79 minor disruptions was Op Falcon. This was launched in May 2022 and is a collaborative effort involving the prevention of cash-based money laundering, particularly the transport of large sums of criminal cash on the roads. In February, approximately £100,000 in cash was recovered after patrols stopped a car, this resulted in two arrests.

Analysis

E1a Money laundering and asset recovery (MLAR) (cash confiscation/cash seizure/recovered assets) is classed as illicit finance on APMIS.

In Q4 (January - March), there were a total of 865 disruptions.

- 45 major disruptions - 44% decrease (-35) in comparison to Q3 25/26
- 206 moderate disruptions - 11% increase (+20) in comparison to Q3 25/26
- 614 minor disruptions - 38% decrease (-378) in comparison to Q3 25/26.

As deadline dates for this report are compressed, the current dataset is likely to be incomplete, it is therefore expected that data will be subject to change and the decrease is partly subject of delayed reporting.

The top 3 disruption types are asset denial & ancillary orders at 62% (691), seizures at 24% (252) and investigative suspect disruptions at 15% (114).

In comparison to the previous quarter (Q3), MLAR disruptions are reporting a 31% decrease (-393). In comparison to the same quarter for the previous year (Q4 24/25), there has been a 22% decrease (-245) in MLAR disruptions.

The benchmark from 24/25 is 4,120, for Q4, disruptions are 6% (+255) above the benchmark target.

Response

Currently focus has been on The Asset Management Office (AMO) for Policing development. This involves supporting the design for ARIT but there are timeline delays regarding system design with Police Digital Service and the supplier.

A short term external comms contract is now in place and will support the AMO 12-month tactical media plan and supporting Knowledge Hub development and LinkedIn. www.AMO.police.uk domain and supplier contract procured with the website to go live of 31/07/2026.

A contract has been secured to support the creation of policies, processes and procedures for the AMO to support contract development throughout 2026.

There is work underway with the College of Policing regarding the financial investigation and asset recovery updates for Authorised Professional Practice (APP), Police Investigator Program student material and guidance (policy) development for policing and broader law enforcement, which should be finalised by the summer.

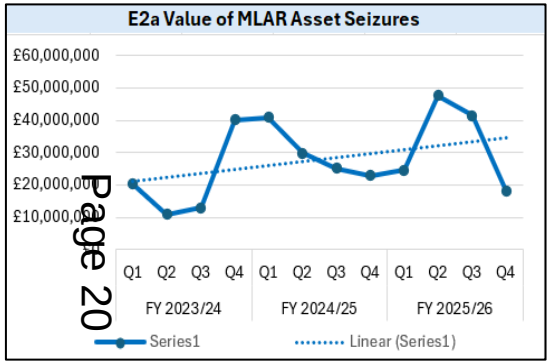
There is also work on Economic Crime Levy growth bids for AMO, Asset Recovery IT Secretariat and Asset Recovery Office.

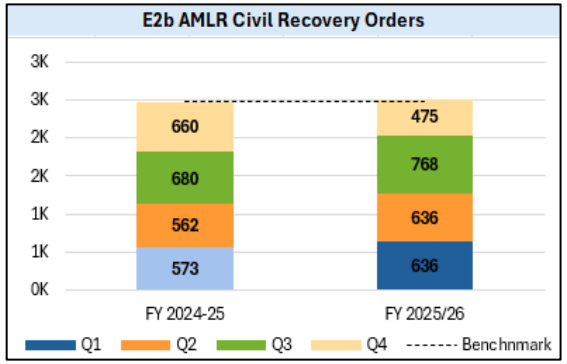
Money Laundering and Asset Recovery

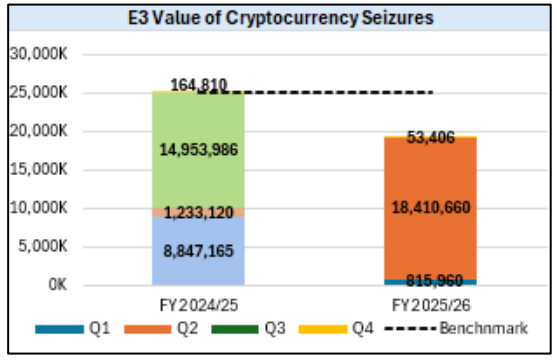
Proactively Pursue Offenders

Performance Measure 2: We will seize and restrain more criminal assets through including released asset denial activity
Performance Measure 3: We will provide training to policing on how to investigate and seize crypto assets. We will ensure accurate records of crypto assets seizures are maintained and provided.

Success Measures:	FYTD Performance	Data Trend
E2a Increase the number of asset freezing orders, restrained assets, and recovered and confiscated assets.		⇩
E2b Increase the number of Civil Recovery Orders.		⇩
E3 Recover a higher number of crypto assets.		⇧







Analysis

E2a In Q4 (January – March), a value of **£18,252,533** asset seizures was recorded for money laundering and asset recovery. In comparison to the previous quarter, this is a **56% decrease** (-£23,151,859). In comparison to the same quarter for the previous year (Q4 24/25), this is an 20% decrease (+£4,629,689). Asset seizures for Q4 are low, however as of Q4, overall asset seizures are reporting **11% above the benchmark** for 24/25 (+£13,104,037). Asset seizures are opportunity-driven, intelligence led and legally constrained which can cause sporadic data trends.

E2b Civil recovery figures in Q4 are reporting a **38% decrease** (-293) in comparison to the previous quarter (Q3) and a 28% decrease (-185) in comparison to same period in 24/25 (Q4). Q4 is reporting **2% above the benchmark for 24/25**, although Q4 was a low month, we are maintaining consistent levels of civil recovery orders.

E3 For Q4, there has been **£53,406** in cryptocurrency seizures, this is 100% increase in comparison to Q3. Q4 is reporting **23% below the 24/25 benchmark** (-£5,919,055).

Response

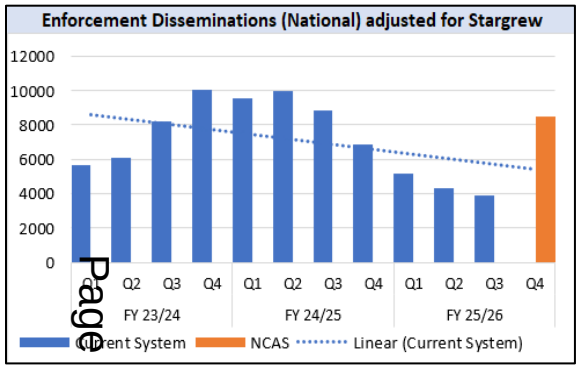
The Asset Management Office (AMO) for Policing development is progressing well. This involves supporting product design of ARIT, however there are timeline delays with product design and suppliers.

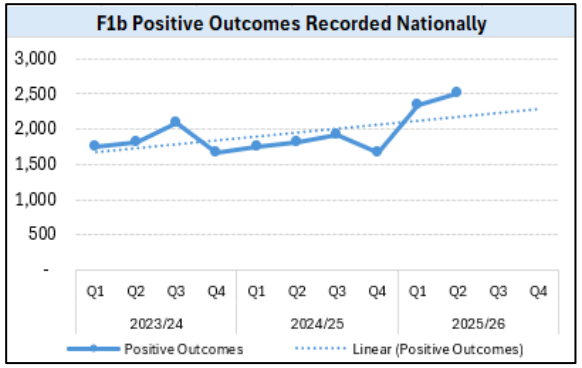
Fraud

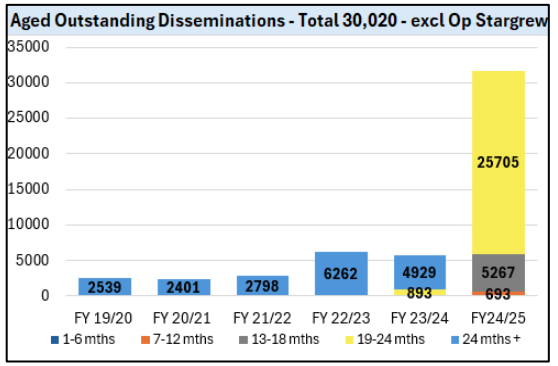
Improve Outcomes for Victims

Performance Measure 1: We will increase the policing response and outcomes linked to NFIB / Report Fraud crime dissemination packages.

Success Measures:	FYTD Performance	Data Trend
F1a Increase the number of Pursue disseminations		⇧
F1b Improve the positive outcome rate		
F1c Reduce the percentage of crime disseminations not yet assigned an outcome		⇧







Outcomes

Q4 2025/26 contained 1 large return from Nottingham, in February 26, an investment Fraud (Op Pennywort), with 75 Judicial outcomes. In working with the National Coordinators Office within CoLP, the MPS are currently conducting a review of their outstanding disseminations and did also return circa 200 separate Judicial outcomes in March 26.

F1a For Q4, there have been **8,524** disseminations, this is a 120% increase in comparison to the previous quarter (+ 4,654). A significant part of this is the automated Call for Service disseminations.

F1b It is not currently possible to establish total outcomes recorded in the quarter as the process for ensuring accurate recording and therefore reporting for both Pre and Post Report Fraud dissemination outcomes is still underway.

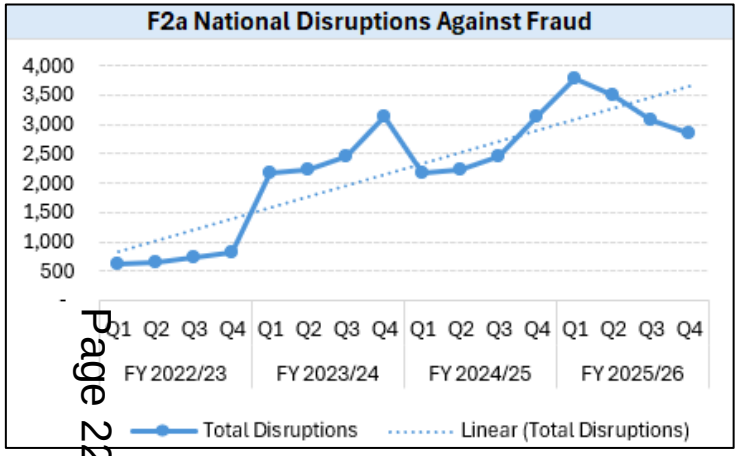
F1c In Q4, there were **30,020** disseminations from 19/20 to 24/25 had not been matched to an outcome. This is **a decrease (which is positive) of 8%** (-2,524) from the previous quarter and an increase of 6% (+1,892) from Q4 24/25. As in F1a, Op Stargrew disseminations have been excluded. A large proportion of these are with a single force and engagement attempts continue to try and reduce this. The next stage of this work is to identify a benchmark for what is a normal proportion of disseminations to be in ongoing investigations under the new Report Fraud work.

Fraud

Proactively Pursue Offenders

Performance Measure 2: We will deliver and co-ordinate regional Proactive Economic Crime Teams and uplifted National Lead Force teams to form part of the National Fraud Squad. The NFS teams will proactively target fraudsters and disrupt offending achieving criminal justice and alternative outcomes.

Success Measures:	FYTD Performance	Data Trend
F2a Increase the number of disruptions against Fraud		⇩



Op Henhouse 5

This intensification took place throughout the month of February and was coordinated by NECC and CoLP. Op Henhouse 5 has reported **172 disruptions for Q4**.

OP ROME - North East Regional Organised Crime Unit

Op Rome involved raising awareness of financial crime amongst business and communities. Messaging was provided direct to employees promoting vigilance around the human element of fraud and common economic attacks. Officers encouraged tactics, behavioural change and understanding of risks. This operation resulted in 115 minor disruptions for Q4, the second largest reported disruption recording for this quarter.

F2a Nationally, there were **2,850** disruptions recorded for Q4 (January - March). Q4 was a low reporting month with a **7% (-224) decrease** compared to the previous quarter. Q4 is reporting a 9% decrease (-283) in comparison to the same period for the previous year. Q1 & Q2 were the highest recorded periods in the last 4 years, these are outliers in comparison to normal levels of disruptions. Disruptions may appear to be on a downward trend; however, these are figures returning to normal levels.

Q4 is reporting **32% above the 24/25 benchmark** (+3,193), therefore, overall disruption performance for the end of the force year is good.

For fraud related disruptions there were:

- 21 major disruptions - 50% increase (+7) in comparison to Q3 25/26.
- 144 moderate disruptions – 6% decrease (-9) in comparison to Q3 25/26.
- 2,685 minor disruptions - 11% decrease (-346) in comparison to Q3 25/26.

Overall, safeguarding is the highest disruption type at 29%, followed by specialist advice at 24%. Investigative suspect disruptions also reported high level disruptions at 18%.

Specialist advice could involve many forms of targeted support or intervention such as educational or behavioural programs. Adult safeguarding involves a referral to the appropriate experts who can support the individual's needs such as social care, health professionals and or legal advice.

Response

Disruption performance has decreased, however overall, is reporting above the benchmark. This will likely see an increase in Q1 from Henhouse results and Op Seraphim activity.

Operational activity is still on-going with Op Seraphim for Q1, The Nigerian pursue activity is set to commence this week, they've been sent 25 packages to action and are carrying out warrants. The UK based pursue activity is largely complete with 27 arrests. Following the Nigerian pursue, there will be engagement with online prevent messaging on social media channels used by threat actors.

The **London Proactive Economic Crime Team (PECT) formally went live on 06/04/26**. It is a collaborative MPS and CoLP unit which is responsible for proactive economic crime with a focus on courier fraud, romance fraud and emerging threats. The unit is pan-London but part of the national (regionalised) PECT network as part of the national fraud squad.

Performance reporting will be via APMIS and for fairness to both Metropolitan Police Service and City of London Police force, will be divided in two each quarter.

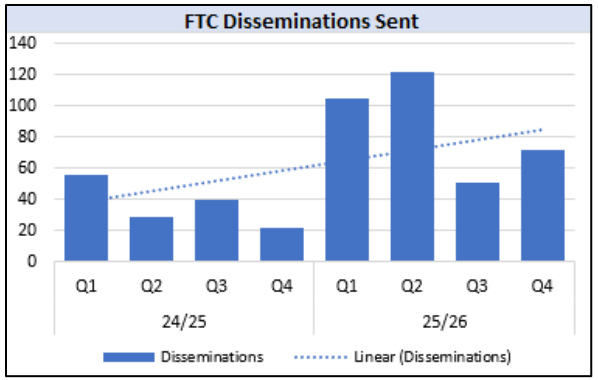
Fraud

Proactively Pursue Offenders

Performance Measure 3: We will lead the National Fraud Squad to PURSUE identified high harm offenders through joint, centrally co-ordinated national operations and to participate in NECC led fraud intensifications throughout the year.
Performance Measure 4: We will support and assist the national development and implementation of the Fraud Targeting Cell by contributing resource and supporting the delivery of systems and processes. We will increase intelligence packages into the system leading to increased proactive operations

Success Measures:	FYTD Performance	Data Trend
F3 Engage in all intensification efforts and target led national operations and evaluate operation-specific outcomes		⇧
F4 Increase the number of Fraud Targeting Cell (FTC) packages allocated, adopted, and investigated		⇧

F3 In Q4, **Op Henhouse 5** took place in the month of February focusing on coordinated pursue and protect activity across all 43 police forces, Police Service of Northern Ireland, Police Scotland, Regional Organised Crime Units, Trading Standards, Financial Conduct Authority and National Crime Agency, Serious Fraud Office and Insolvency Service. Operation Henhouse 5 resulted in the highest number of arrests to date (557), which is a 29% increase on Operation Henhouse 4. Seizures resulted in a value of £27.1m, and 51 successful disruptions were completed against websites, phone numbers, social media accounts and domains. In addition to this, National Trading Standards E-Crime Team removed/ suspended 4,242 URLs. (Uniform Resource Locator – address of a unique resource on the internet, used by browsers to retrieve published resources such as web pages, images and documents). As a result of Henhouse 5 over 4,000 individuals have been the subject of initiatives including safeguarding visits, prevention advice through attendance at local community presentations or training sessions.



F4 In Q4, a total of **72 disseminations** were sent by the Fraud Targeting Cell (FTC). This is a **41% increase** (+21) compared to Q3, and a 227% increase (+50) compared to the same period for the previous year.

The main driver for disseminations were part of Operation Seraphim to both UK and overseas law enforcement. In addition to this operation, there have been other disseminations sent in relation to scam centres, SIM farms, investment frauds, and fraud enabling products.

In January, off the back of an FTC referral, the Nigerian Police Force – National Cyber Crime Centre (NPF-NCCC) executed a warrant resulting in the arrest of 7 subjects linked to a sophisticated scam operation in Nigeria targeting the UK and US through investment scams using META platforms. In addition, East Midlands Serious Organised Unit PECT located and arrested an outstanding subject of an FTC Test Phone intelligence package disseminated.

Response

Op Seraphim

Progress on Op Seraphim has been made with intelligence products relating to cybercriminals advertising fraud enabling products on Telegram channels. Currently work is on-going with Nigerian law enforcement and the Proactive Economic Crime Team (PECT) network. Close work is also on-going with the Cyber Defence Alliance to identify and attribute the cybercriminals.

Fraud Targeting Cell alongside the PECT Coordinator, have been having discussions with Flashpoint, a Cyber Threat intelligence company, around assisting in the attribution of the entities to cybercriminals.

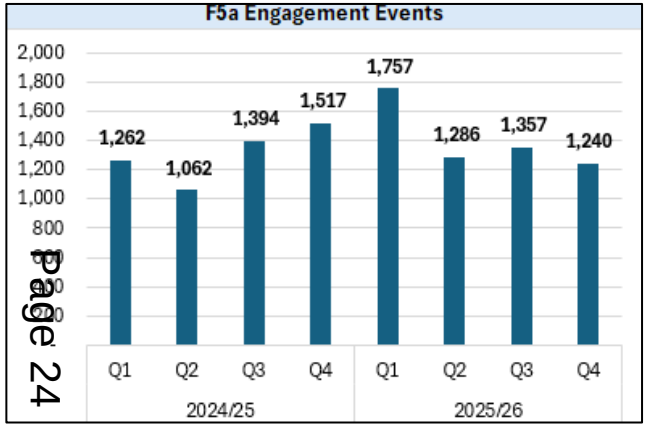
The Nigerian pursue activity is set to commence in Q1, they've been sent 25 packages to action and are carrying out warrants. The UK based pursue activity is largely complete with 27 arrests. Following the Nigerian pursue response, we'll be engaging with some online prevent messaging on social media channels used by threat actors.

Fraud

Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

Performance Measure 5: We will develop and deliver a centrally co-ordinated National Fraud PROTECT Network that will align with the National Cyber PROTECT Network, share best practice, and promote local delivery of national messaging.

Success Measures:	FYTD Performance	Data Trend
F5a Increase the number of Protect engagement events and attendees		⇩
F5b Percentage of protect engagement event attendees satisfied with the engagement they attended		⇧
F5c Percentage of protect engagement event attendees likely to change their behaviours as a result of engagement		⇧



F5a For Q4, **1,204 engagements** were held across the network, with **52,359 attendees**. Q4 is reporting a 9% (-117) decrease in comparison to the previous quarter and a 18% (-277) decrease on Q4 24/25. For attendees, Q4 is reporting a 79% decrease on Q3. (-195,512)

F5b&c The fraud protect surveys continue to be adopted by the national Fraud Protect Network during their presentations, events and interactions with citizens and businesses across the country.
In Q4, **98%** were very satisfied and satisfied with the event/engagement (2% increase from Q3)
99% were likely to change their behaviour or already undertake that behaviour (2% increase from Q3).

In Response
Report Fraud Protect have taken responsibility for the national training products around Technology Facilitated Abuse. Working closely with the National Cyber Security Centre (NCSC) National Police Chiefs Counsel lead (NPCC) and Home Office, Report Fraud Protect will ensure all the resources remain relevant and up to date and will promote delivery to public protection teams and advocacy groups across the UK. Working closely with local Forces and Regional Teams hosting a Working Group, where best practice is shared. The Guidance document has been updated by NCSC and circulated. It has been agreed the Report Fraud Working Group will be the conduit from which all future changes will be made. A PowerPoint will be used to deliver presentations to charities, advocacy groups, and Public Protection Teams.

Report Fraud Protect Services hosted the annual National Protect Conference during February. The conference brought together the fraud and cyber protect network, the conference hosted 250 people from Fraud, Cyber and our stakeholders across the nation including NCSC and National Crime Agency. The release of Report Fraud was also covered and led to meaningful conversations about the collaboration across the network.

In March, Report Fraud Outreach and Engagement Team presented to 140 delegates at the VisaV Limited National Community Engagement Conference. They spoke about the new Report Fraud Service and how Report Fraud Alert is helping to deliver effective protect messaging and drive meaningful behavioural change. Report Fraud Alert uses the VisaV platform to communicate information on emerging fraud and cyber crime threats to over 950,000 subscribers across the UK.

For Q1, The Home Office has tasked the protect team to create a booklet catered to International Students around fraud and cyber awareness. Work is ongoing with universities as well as the Protect Network to build this booklet, and a draft is currently with the Universities and Network for feedback before going through the final design and draft stage. The finished booklet should be released at the start of Q1.

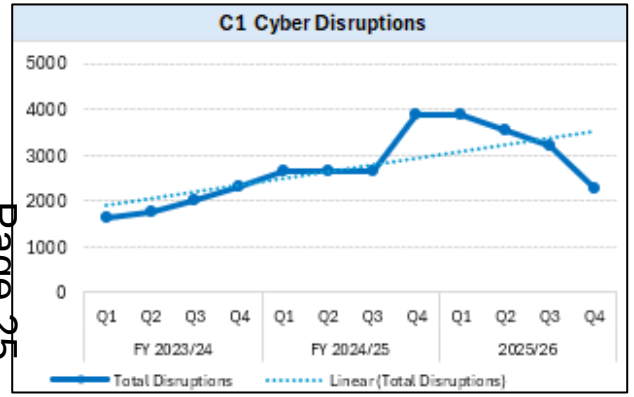
Alongside the IDT team, the team have also been asked to help with the hosting of the annual Courier fraud summit, which was previously hosted by Barclays. This is currently in progress.

Cyber

Improve Outcomes for Victims

Performance Measure 1: We will increase the policing response and outcomes linked to NFIB / Report Fraud crime dissemination packages. We will ensure full and timely compliance from forces to record disseminations from the NFIB appropriately and that subsequent outcomes are reported back to NFIB correctly.
Performance Measure 2: We will increase intelligence led proactive operations and self-development operations regarding Computer Misuse Act offending, ensuring the relevant deconfliction safeguards are followed.

Success Measures:	FYTD Performance	Data Trend
C1 Increase the number of disruptions against cyber crime		⇩
C2 Increase the number of operations involving the Computer Misuse Act (CMA)		⇩



C1. In Q4 (January- March), there were a total of **2,272** disruptions.

- 2 major disruptions - 50% decrease (-2) in comparison to Q3 25/26
- 92 moderate disruptions - 28% increase (+20) in comparison to Q3 25/26
- 2,178 minor disruptions - 30% decrease (-944) in comparison to Q3 25/26.

In comparison to the previous quarter (Q3), Cyber disruptions are reporting a **29% decrease** (-926). In comparison to the same quarter for the previous year (Q4 24/25), there has been an 42% decrease (-1,628).
Disruptions appear to be on a downward trend however; Q4 24/25 - Q2 25/26 were outliers and exceptionally high quarters. For Q4, disruptions are reporting **9% (+1,019) above the benchmark.**
The top 3 disruption types are specialist advice at 76%, training at 24% and safeguarding at 7%. Specialist advice could involve many forms of targeted support or intervention such as educational or behavioural programs. Adult safeguarding involves a referral to the appropriate experts who can support the individual's needs such as social care, health professionals and or legal advice.

C2. For Q4, there have been no Vulnerability Notification Packs or Malicious Notification Packs (that informs an organisation about potential weakness in its systems or an alert of malicious behaviour detected on the network such as attempted intrusions) distributed to national and regional Cyber Crime Units. These should resume before the end of Q1 2026/27.

Response
One significant reason for the reduction has been a result of a national review by the NPCC APMIS team, the purpose of which is to improve the quality and consistency of disruption reporting. The review found that disruptions often recorded effort, rather than the required impact police activity has had on serious and organised crime. The review is likely to lead to further challenge around disruption recording through 26-27.
The Fraud Intelligence Cell is now firmly established and operating at pace, with contracted private industry partners actively identifying and developing proactive intelligence opportunities across the fraud threat landscape.

Project Capstone contracts are in place through to April 2027, providing medium-term continuity and capability assurance. The procured technologies and services will enable the continued delivery of Project Capstone's core objectives, specifically enhancing law enforcement's ability to identify and prioritise high-harm offenders who utilise cryptocurrency as a payment mechanism for illicit goods and services. This procurement ensures sustained access to specialist expertise and tooling that are critical to responding effectively to evolving criminal use of digital assets.

Under Project Capstone, the NPCC has successfully completed the procurement of advanced blockchain analytics and threat intelligence tools, alongside specialist support from private industry partners. During Q4, private industry partners generated **46 intelligence packages**. Of these, 14 packages were disseminated to regional teams for operational action, with the remaining products undergoing further development or assessment. This demonstrates a growing pipeline of actionable intelligence and collaboration between the Capstone team and industry specialists.
Private industry partners supporting Online Serious Organised Crime (SOC) activity produced 22 intelligence packages during the last quarter.
Of these, 4 packages have been disseminated to regional teams for operational consideration, with a further 15 packages currently under development and exploitation by the NPCC Capstone team. This reflects a structured and maturing intelligence workflow, supporting the identification and disruption of organised criminal activity facilitated through online platforms and digital payment mechanisms.

Cyber

Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

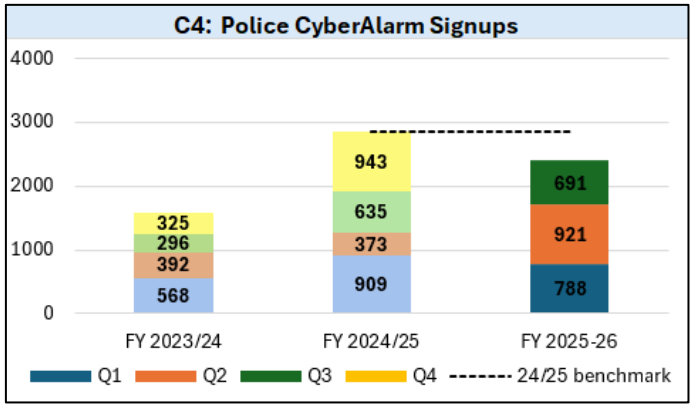
Performance Measure 3: We will develop the current PROTECT notification processes to ensure a consistent approach to both the direct PROTECT officer taskings and the notifications delivered at scale.

Performance Measure 4: We will ensure ROCUs and Forces are regularly using Police Cyber Alarm to help support member organisations when issues are identified and use the data to inform and drive PROTECT, PREVENT and PURSUE activity. PROTECT Officers will promote Police Cyber Alarm to all SME organisations they engage with.

Success Measures:	FYTD Performance	Data Trend
C3 Increase PROTECT notifications issued to victim organisations.		⇨
C4 Protect Officers to promote Police CyberAlarm to SME organisations.		⇧

C3 A Protect Notification is a method used to notify victim organisations when intelligence is received indicating a cyber crime has occurred or is likely to occur against their IT system. If the intelligence suggests a live cyber security threat where quick time actions are needed, then it will be treated as urgent and the NCA TICAT team (Triage, Incident, Coordination and Tasking) will deliver the notification via phone, or via the Protect Network for a same day in-person visit to the premises.

During Q4, the network reports 166 taskings, of which 143 (86.1%) were completed within the quarter. Protect Notification outcomes are captured, helping to improve the recording of cybercrime in the UK and quantify the impact of the Protect network. Currently the network sits at **94.7% for the year compliance with March '26 returns outstanding**. Q4 25-26 has seen a significant increase in Protect Notifications being tasked out to regional protect teams for completion.



C4 In Q4, 0 Small to Medium-sized enterprises (SMEs) signed up to Police Cyber Alarm.
Overall, performance is reporting **16% below the 24/25 benchmark** (-460).

Please see response section.

Response

Police CyberAlarm (PCA) is changing its supplier to Waterstons Ltd. The system was temporarily paused on 28 February 2026. PCA continue to receive expressions of interest, and work is ongoing with the Department for Education. Under the Risk Protection Agreement (RPA), schools will be required to register with PCA.

The new system has completed User Acceptance Testing (UAT) and is now awaiting external penetration testing before going live.

The new system will no longer need a data collector to receive vulnerability reports. This means more businesses can take part, provided they have a publicly accessible website or a static IP address.

PCA have managed communication with previously registered members through a new Customer Relationship Management (CRM) system.

Preparation for marketing the new system has begun, supported by an external marketing company.

The wider cybercrime network was briefed during Q4 at both Team Cyber UK and the National Protect Conference.

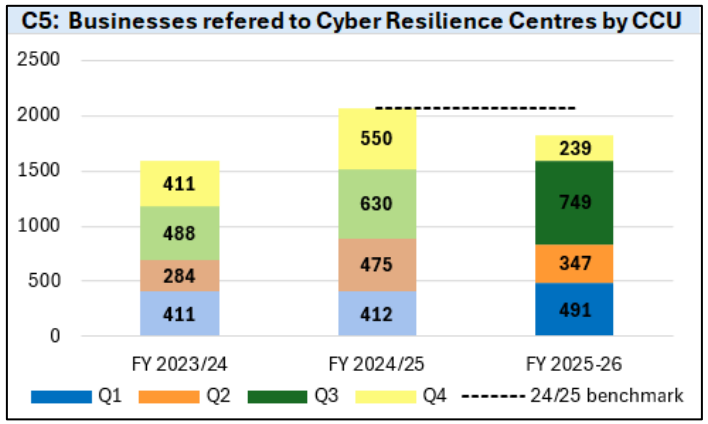
Waterstons Ltd are developing a brand-new, custom-built system for Police CyberAlarm which will deliver improved and increased functionality. The new system is expected to be launched in Q1 of 2026-2027. However, until this available, one of the functionalities that has been disabled are Notification Packages for law enforcement. Member organisations are still able to register, download, install and configure the current system which enables them to receive their monthly threat and vulnerability reports.

Cyber

Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

Performance Measure 5: We will deliver the new NPCC Cyber Resilience Centre (CRC) Model. This includes the new Operating Model to deliver the levels of consistency and assurance required. CRCs and PROTECT officers will work together to support each other's work and grow CRC membership

Success Measures:	FYTD Performance	Data Trend
C5 Increase the number of Cyber Crime Unit referrals to Cyber Resilience Centres (CRC)		⇩



C5
In Q4, the number of Cyber Resilience Centre (CRC) referrals **decreased by 68%** (-510) in comparison to the previous quarter.

Overall, figures are reporting **12% (-241), under the benchmark for 24/25.**

Response
Referrals from Protect officers into the Cyber Resilience Centre Network reduced markedly in Q4, falling from 749 in Q3 to 239. This reduction should be considered in the context of a period of **significant structural transition** across the CRC Network, rather than as an indicator of reduced underlying demand.

Q4 coincided with the final phase of the national restructure, including consolidation of regional entities, changes to governance arrangements and the alignment of delivery models under a single national operating framework. As the restructure nears completion and the reconfigured Customer Relationship Management system is implemented, referral pathways are expected to stabilise and scale, supported by clearer national governance, improved visibility of outcomes and enhanced ambassador activity, enabling referral volumes to recover while improving conversion and impact for Small to Medium Enterprises.

The new Key Performance Indicators for the network are under consultation with key partners, but are likely to be:

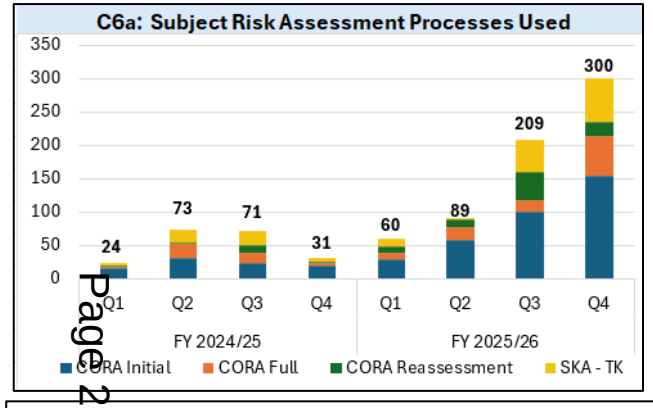
1. Membership growth (particularly in priority sectors)
2. Number of 30 minute 'cyber health checks' completed
3. Number of referrals to, and engagement with, the NCSC Cyber Action Toolkit (CAT)
4. CRC members taking up Cyber Essentials/Cyber Essentials +
5. Conversion of membership to Cyber PATH services

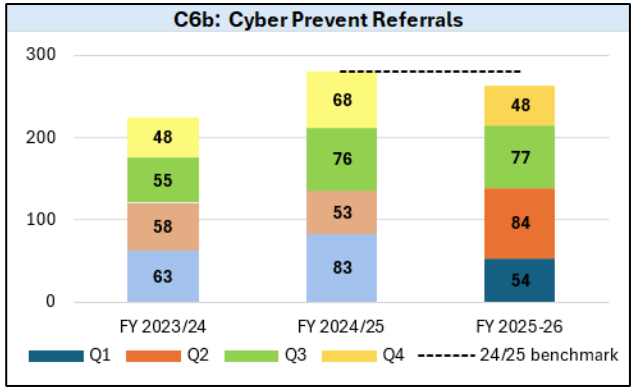
Cyber

Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

Performance Measure 6: We will develop improved referral process for new nominals - to include Target Operating Model and definition of when a referral should be made. We will introduce a single national or regional referral mechanism and implement risk assessment (CORA) and tasking mechanisms for PREVENT referrals.

FYTD	FYTD Performance	Data Trend
C6a Increase the number of CORA assessments made		⇧
C6b Increase the number of PREVENT referrals		⇩





C6a A CORA assessment is used to assess the risk posed by individuals referred and helps determine the level of cyber capability from skills, knowledge, and access to technology. This helps decision making in deciding the appropriate intervention, diversion, or support to proceed with. For Q4, risk assessments have **increased by 44%** (+91) in comparison to Q3 and is reporting **231% (+459) above the 24/25 benchmark.**

During Q4, activity continued to focus on three principal areas:

1. Completing CORA for all accepted referrals
2. Creating a robust evidence base to demonstrate impact
3. Addressing cross-cutting thematic areas across the business, specifically CT and COM

At the start of the year, there was a reduction in both referrals and CORA completion. This was directly linked to uncertainty around the future retention of Cyber Prevent and the resulting decision not to recruit into vacant posts.

C6b A total of **48 Cyber Prevent** referrals were received in Q4, an **38% (-29) decrease** from Q3 and Overall, Q4 is reporting **6% below the benchmark** for 24/25 with a total of 263 referrals for the year.

Response

Following the reduction in assessments due to the uncertainty of Cyber Prevent, activity has increased significantly, ultimately exceeding performance levels seen in previous years. This improvement coincided with the introduction of the formalised Counter Terrorism (CT) referral process and the establishment of Supervisor Governance Meetings. These meetings have proven critical in providing both accountability and support to managers in relation to Prevent activity. They have also been paramount in increasing both the volume and quality of referrals, as well as enabling the sharing of good practice across teams.

The implementation of CORA has now been fully completed. This provides the ability to better understand risk across the network and assess which interventions are most effective. It is proposed that an evaluation of CORA is undertaken jointly with the Home Office, with the intention that learning can be shared with international cyber law enforcement partners and applied across other crime types.

In January 2026, work on the reoffending rate of cyber nominals was completed. This was a joint piece of work involving the NPCC Cybercrime Team, National Cyber Crime Unit and Cambridge University, covering the full duration of the programme to date. The findings demonstrate that the programme and associated interventions have been highly effective. As a result, the approach is now being considered by other programmes, including Cohort Offender Management.

The CT referral process is now fully embedded. Referrals from CT have increased, driven by greater confidence that risk is being appropriately identified, managed and governed. We are now going to evaluate the process. Prevent activity will now extend into COM. A dedicated training package is currently being developed to support staff, with a particular focus on Prevent practitioners.

In addition, the new Prevent lead will also act as the embedded liaison with the Rhyobasalt Intelligence Coordination Cell (RICC), which manages the COM threat. This model is viewed as an effective mechanism for delivering against the 3rd aims and strengthening integration across relevant business areas.

Cyber

Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

Performance Measure 7: We will roll out the Cyber & Digital Specials & Volunteers (CDSV) Programme and platform to every region and Force and ensure effective management and utilisation of CDSV skills across the network.

FYTD	FYTD Performance	Data Trend
C7 Increase the number of CDSV Programme participants and their utilization across the network.		⇨

C7 For Q4, there remain **146 volunteers** recorded on Assemble, across 35 teams. The full time National Lead and Deputy Lead roles now filled, awaiting CoLP Kit and for deputy role, vetting completion to start on secondment with CoLP. Initial identification of strategic national volunteers to work nationally in support of the Lead and Deputy Lead's strategy and delivery paused whilst awaiting postholder to commence.

In Q4, **Volunteers logged 387 hours of work**. A key element of the new strategic plan is to understand the barriers to recording activity and to develop a more robust way of monitoring performance. Commendations from the Commissioner of the City of London Police were awarded to 2 volunteers for their exceptional work with the North Wales Cybercrime Unit

Response

Volunteer consultation on new branding Cyber Digital Specials and Volunteers (CDSV) network to reflect wider scope beyond cyber, to the Specialist Crime Volunteer Network has been sought. The team is working with the NPCC Science & Technology team and Regional Science & Innovation Managers to embed the use of volunteers within the NPCC strategy.

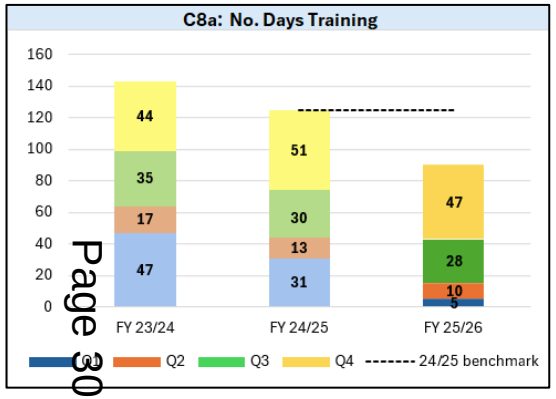
A 12-month project plan is being drafted to capture initial national deliverables for the National Lead and Deputy roles aligned to the Cyber and Fraud strategy objectives.

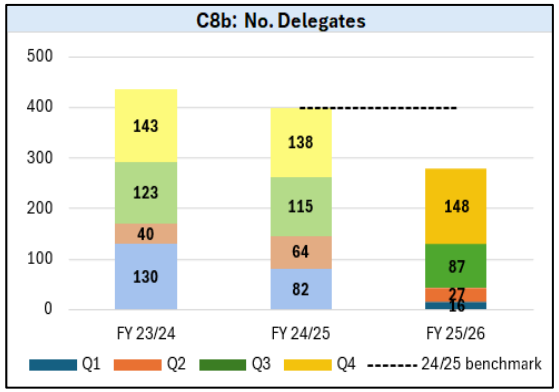
Cyber

Improve Outcomes for Victims

Performance Measure 8: We will revise and roll out a clear training, CPD and accreditation pathway for all roles within TCUK, with regular reviews of the training needs analysis and advancements in technology / threats. NPCC Deliver new strategy and delivery with the Economic and Cybercrime Academy.

Success Measures:	FYTD Performance	Data Trend
C8a Increase the number of Cyber training days		⇧
C8b Increase the number of Cyber training delegates		⇧





C8a For Q4, there has been a **68% increase** (+19) in the number of formal training days provided in comparison to Q3. In comparison to the same quarter for the previous year (Q4 24/25), there has been an **8% decrease** (-4). Q4 is reporting a strong improvement in comparison to previous quarters for force year 25/26, however overall, training days are reporting **28% below the benchmark** (-35). Although reporting below the benchmark, delegates and training days have both reported large increases in Q3 & Q4.

C8b During Q4, **148 delegates** were delivered formal training courses, this is a **70% increase** (+61) in comparison to Q3 and a 7% increase (+10) when compared to the same period for the previous year (Q4 24/25). Overall, Q4 is reporting **30% under the benchmark** (-121).

Response

The Critical Incident course has now completed its pilot phase and has been formally signed off. Feedback has been extremely positive across participating Forces, ROCUs and the NCA.

A tendering process is currently underway to appoint the training provider for the 2026/27 period, covering a three-year term.

The NeuroVision programme is designed to support practitioners working with neurodivergent victims, witnesses and suspects. The NeuroVision Managers' course focuses on equipping managers to effectively support and supervise neurodivergent staff.

Analysis has shown that neurodivergent staff are proportionally more represented within the Cybercrime Network than within general policing and the wider population. Findings from the National Cybercrime Network Survey (conducted biennially) show very positive feedback regarding the value and delivery of both NeuroVision courses.

The SudoCyber contract has been extended until December 2026, with a significant discount successfully negotiated. In addition to the core platform, SudoCyber continues to deliver monthly CPD events and has recently implemented substantial enhancements to its operating ecosystem. A review of the metrics and the outcomes in relation to the platform is ongoing to give great insights. Key platform updates include:

A redesigned dashboard offering real-time visibility of learner progress, organisational rankings, activity trends and achievements through dynamic widgets, statistics and badges.

Improved course and competition access, using rotating widgets, flexible list views and curated featured content.

Introduction of **SudoRanger**, an AI-powered learning assistant embedded within labs, providing contextual guidance, summaries of learning materials and real-world examples while encouraging independent problem solving.

Enhanced lab usability through a redesigned sidebar, an upgraded notifications system for achievements, completions and events, and expanded learner feedback mechanisms to support continuous improvement.

The NPCC cybercrime training DI and the Rhyobasalt Intelligence Coordination Cell (RICC) embed from the Team have been tasked with developing a training package for staff to create awareness of the COM threat. They are in the process of developing an online lab to support cyber and non-cyber staff.

National Lead Force
City of London Police Performance Report

FY 2025/26
Q4: January – March 2026

Executive Summary

It is only possible to report a partial outcome picture for Q3 and Q4 as changed to processes since Report Fraud's introduction mean like for like data is not currently available.

Even with partial information available due to the positive outcomes of 2 significant operations in Q3 COLP has exceeded the service level in the 12 months to date compared to the last financial year.

It is also not possible to report on the national reporting service metrics relating to victims and vulnerable person alerts for this reason.

A significant increase in Economic Crime Academy delegates was seen in Q4 as is seasonally seen however due to the challenges seen earlier in the year (FQ1 and FQ2) the service level set for the year has not been met.

City of London Police has met all of the required service levels set for this financial year across, Offender disruptions, asset seizures and disruption to enablers.

Whilst minor decreased were seen in Q4 performance remains above the level for the past 12months.

CoLP also continued to support national intensifications to both target offenders and increase protect activity this quarter.

A more sustained approach intensification is being progressed for the year 26/27.

Following the introduction of Report Fraud the growth in Prevention and Disruptions both in terms of practical removal of enablers and from social media impressions for more traditional protect have seen a significant increase.

It is hoped that these increases will be sustained as the new system and processes embed further.

Performance Assessment

The dashboard provides an assessment of City of London Police performance against the objectives set out in the **National Policing Strategy for Fraud, Economic and Cyber Crime 2023-28**. The National Policing Strategy was launched in November 2023 and translates national strategies and objectives set by His Majesties Government into actionable measures for policing in the areas of fraud, money laundering and asset recovery and cyber. The report shows CoLP attainment against the objectives. The National Policing Strategy sets out a purpose to "improve the UK policing response to fraud, economic and cyber crime" through three **key cross cutting objectives** of:

- Improving outcomes for victims;
- Proactively pursuing offenders;
- Protecting people and business from the threat of Fraud, Economic and Cyber Crime.

The NLF plan sets out **key cross cutting enabling commitments** that City of London Police is seeking to achieve:	**FYTD Performance**	**Data Trend**
We will deliver and co-ordinate regional Proactive Economic Crime Teams and uplifted National Lead Force teams to form part of the National Fraud Squad. The NFS teams will proactively target fraudsters and disrupt offending achieving criminal justice and alternative outcomes.		⇩
We will deliver enhanced victim care & support to victims of fraud & cyber crime, to reduce harm of offending and prevent re-victimisation.		⇩
We will deliver agreed and consistent content across the PROTECT network, to ensure consistent messaging in line with HMG guidance and promoting HMG systems and services.		⇧
We will improve the policing response to fraud. Report Fraud objectives will be added when the system launches.		
We will increase the policing response and outcomes linked to NFIB / Report Fraud crime dissemination packages		⇧
We will lead the National Fraud Squad to PURSUE identified high harm offenders through joint, centrally co-ordinated national operations and to participate in NECC led fraud intensifications throughout the year.		⇩
We will upskill and train our staff so that they are able to effectively respond to the threat of fraud, economic and cyber crime.		⇧
We will develop and action a National Economic Crime Workforce Strategy.		⇧

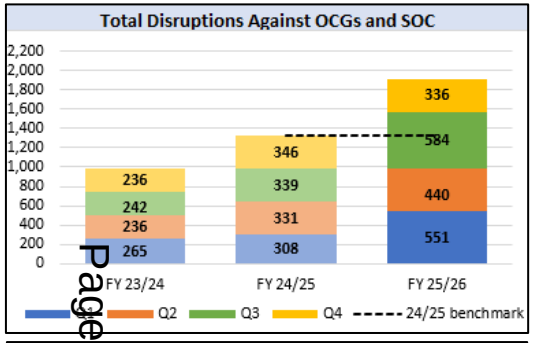
National Lead Force Fraud Operations: Includes National Fraud Squad Teams and Funded Units

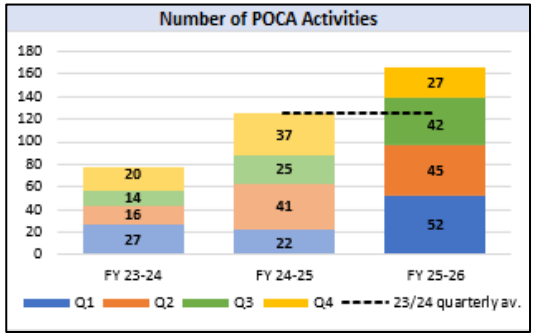
Proactively Pursue Offenders

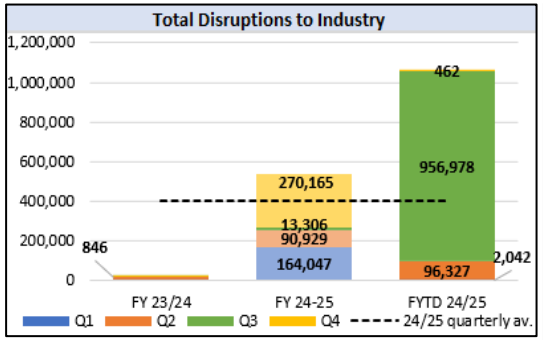
We will deliver and co-ordinate regional Proactive Economic Crime Teams and uplifted National Lead Force teams to form part of the National Fraud Squad. The NFS teams will proactively target fraudsters and disrupt offending achieving criminal justice and alternative outcomes.

Success Measures:

A. Increase the number of disruptions against fraud organised crime groups (OCG) and serious organised crime (SOC)
B. Increase the number of POCA activities
C. Increase the number of disruptions against technological enablers







OCG Disruptions

In Q4 teams recorded 80 disruptions against OCGs:

- **2 major** disruptions (0 change on Q3)
- **17** moderate (-9 from Q3)
- **61** minor disruptions (-3 from Q3)

Overall disruptions are reporting a **42% decrease** in comparison to Q3 (248), however overall figures are reporting disruptions at **44% over the 24/25 benchmark.**

Financial Disruptions

In Q4 25/26 Fraud Teams reported **27** POCA activities down **36% (-15)** from Q3 and 33% (+41) above the 24/25 benchmark.

These had a value of **£6,800,00** up **31% (+£1,628,615)** from Q3 and up 255% (+£4,886,499) from the 24/25 benchmark.

Activities included: **7** confiscations, **3** asset restraining orders, **20** cash detentions and **8** cash forfeitures.

Industry Disruptions

In Q4 Fraud teams reported:

- **250** disruptions to websites
- **212** to cards and bank accounts
- **0** to social media and other

Overall disruptions are reporting 95% over the benchmark for 24/25, however Q4 is reporting a 99% decrease from Q3.

Response **Industry Disruptions**

There is no narrative response to this metric at this time

Response **OCG Disruptions**

Op Henhouse was the largest operation for this quarter which reported many success stories such as DCPCU reporting 31 APMIS disruptions, 31 arrests, £162,000 asset freezing orders and £427,000 seized from a bank account believed to be money laundering.

PIPCU reported 42 SOC disruptions for Q4 alongside 8 arrests, £550,000 in noncash seizures and £614,000 in asset freezing orders as part of Op Henhouse 5.

PIPCU Officers executed warrants at a distribution warehouse in Lancashire uncovering counterfeit weight-loss drugs, including fake Ozempic, Mounjaro, and Retatrutide – an unauthorised product not approved for medical use.

Financial Disruptions

Eight defendants were convicted of money laundering from an ART investigation. This was related to receipts of funds from fake trade-in-submissions for Apple iPhones to EE's appointed recycling company. One defendant has been subject to a Compensation Order and the remaining confiscation investigations are on-gong.

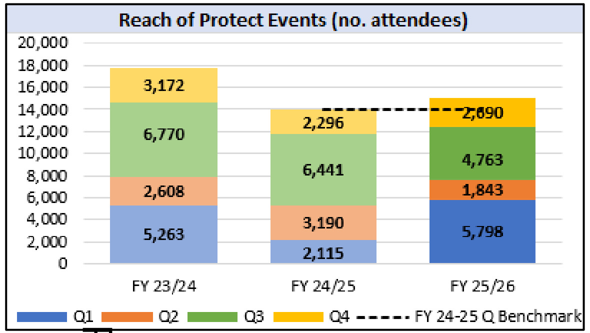
An ART confiscation investigation of Conspiracy to defraud, concluded with the following Orders being made against a nominal who had a criminal benefit of £1,417,139.18 and an available amount of £22,673.00 and another nominal who had a criminal benefit of £467,490.18 with an available amount of £1,562.30.

National Lead Force Fraud Operations: Includes National Fraud Squad Teams and Funded Units

Protect People and Businesses

We will deliver enhanced victim care and support to victims of fraud and cyber crime, to reduce harm of offending and prevent re-victimisation. We will deliver agreed and consistent content across the PROTECT network, to ensure consistent messaging in line with HMG guidance and promoting HMG systems and services.

Success Measures:		
A. Increase the number of protect engagements and attendees		⇩



Protect Events

- Teams held **62** events in Q4, down 13% in comparison to Q4 24/25 **(-13)**
- **2,690** people attended these events up 17% from Q4 24/25 **(+394)**
- Activity peaked in February with **34** events & **1,717** attendees. Overall reach is reporting 8& above the benchmark (+1,052)

<u>Response</u> Protect Events

The Insurance Fraud Enforcement Department (IFED) have had a productive Q4, to which they visited the Bulgarian Embassy to share knowledge and intelligence about IFED and insurance fraud in the UK amidst the rise of insurance fraud in Bulgaria. IFED also delivered a case study on bringing fraudsters to justice entitled effectively utilising evidence to drive the quality of stakeholder investigations and referrals.

A visit the Metropolitan Police Service was also completed to advise around taxi insurance fraud, particularly a rise in fraudulent documentation.

The Police Intellectual Property Crime Unit (PIPCU) have focussed on highlighting the benefits of Public Private Partnerships and the significant benefits of cross border international investigations. PIPCU held meetings held with the Anti-Slavery Collective; Foreign Law Enforcement Community Group and the Scottish Anti-illicit Trade Group have led to stronger relationships and the development of campaigns targeting the most vulnerable in the Intellectual Property Crime Eco-system.

In the rapidly developing field of Digital Piracy, PIPCU have presented to International experts at the IPTV Taskforce and other Private industry parter groups which has strengthened relationships, garnered expertise and shared valuable information.

Working closely with the Intellectual Property Office (IPO), PIPCU have also assisted in presenting to delegations from South America, India, Pakistan and Uzbekistan, Sharing experience on international Intellectual Property investigations, techniques and best practice.

In Response

In 2024/25 NFIB Protect worked with the National Cyber Security Centre and Age UK on a project to deliver 'how to stay secure online' training to selected Age UK centres. A collaborative slide presentation was produced and shared with ROCUs to deliver within 16 Age UK areas. The project is continuing into 26/27 with an updated presentation being provided to the Regional Organised Crime Units (ROCU).

Report Fraud Protect have hosted continued professional development events which form a key part of our service and a survey asking the network for suggestions will be distributed. The first of these (on-line harm networks) presented by Dr. Benjamin Lee were delivered on two dates, 18th and 25th March with a total of 131 attendees.

There is ongoing work which continued to evaluate the results and effectiveness of Project Aegis. This a review of how fraud protect work was being carried out was undertaken. This is leading to a more focussed effort in the protect engagement and tactics to be undertaken. It is therefore likely that this will lead to lower volumes of engagement events in future quarters, but with a greater impact of the advice received.

For Q1, the CoLP Protect team will be collaborating with the Home Office in development of a standardised presentation aimed at the Charity/Civil Society Organisation sector which aims to promote fraud and cyber awareness at an organisational level. The project is still in the early scoping stages, with collaboration ongoing with the Home Office Crime directorate, Charity Commission, National ROCUs as well as the Charity Sector.

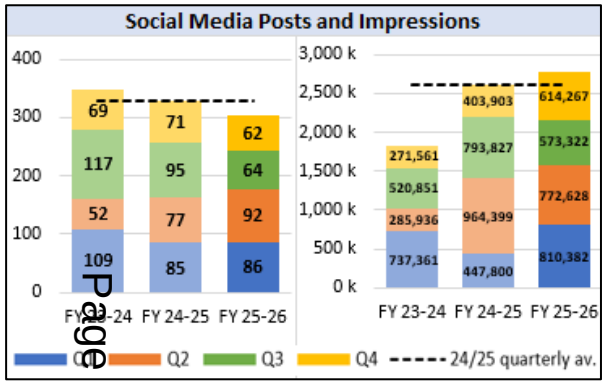
National Lead Force Fraud Operations: Includes National Fraud Squad Teams and Funded Units

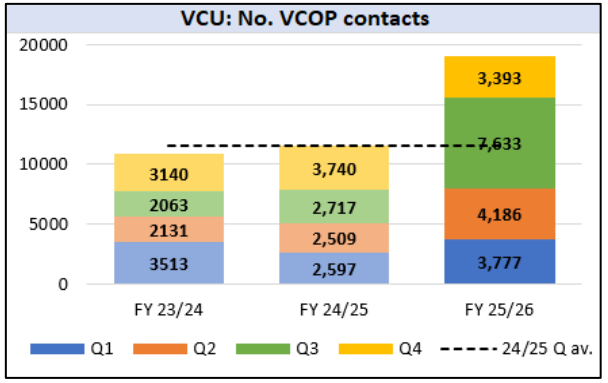
Protect People and Businesses

We will deliver enhanced victim care and support to victims of fraud and cyber crime, to reduce harm of offending and prevent re-victimisation. We will deliver agreed and consistent content across the PROTECT network, to ensure consistent messaging in line with HMG guidance and promoting HMG systems and services.

Success Measures:

B. Increase the number of social media posts and impressions
C. Increase the number of Victim Care Unit contacts





Social Media

Teams posted **62** messages on social media, down **9% (-9)** on Q4 24/25. The related impressions increased to **614,267**, up **52% (+210,364)** on Q4 24/25. Impressions are 6% over the 24/25 benchmark.

Response **Social Media**

Report Fraud launched the campaign 'Every Report Counts' and focused on romance fraud awareness for February. Activity from Report Fraud has been reduced for this quarter whilst focus remains on the Report Fraud launch.

Victim Care Unit

VCU was responsible for **17,772** victims in Q4 up **3% (+547)** victims since Q3 relating to **85** (+2) investigations. A total of 3,393 VCOP updates were issued, down **113% (-4,240)** from Q3. **20,527** victims received additional Protect advice

Response **Victim Care Unit**

As a result of a policy change at the start of the quarter, VCOP outreach hit 3,393 with a further 20,527 victims being offered one time protect advice, some being within the service however 18,400 victims were as part of Operation Queby on behalf of Romanian Police, who had an identified many UK victims for a crypto investment scam.

Social Media

PIPCU issued posts regarding an international operation targeting illegal streaming services with seven different countries. PIPCU have also issued several posts about Internet Protocol Television cases (ITVP), one notable in February, involving a 750k worth of IPTV servers being shut down.

The Insurance Fraud Enforcement Department (IFED) **IFED** activity peaked in January with an arrest regarding a male with a long history of fraud offences sentenced to two years in prison. IFED also collaborated on a joint investigation with the Metropolitan Police Service involving tens of thousands of potential victims affected by spoof insurance apps, this resulted in five arrests.

DCPCU (Dedicated Card and Payment Crime Unit) was mentioned on Radio Suffolk and praised by Giles Mason for the work DCPCU completed preventing 63 million pounds of fraud being stolen in 2025.

COLPS National Lead Force Operations Teams issued a press release regarding Operation Henhouse which was supported by Good Morning Britain covering a fraud ops warrant with Lord Hanson (Minister for Fraud). There have also been several press releases for Q4 involving several fraudsters such as a male who targeted other males on dating apps.

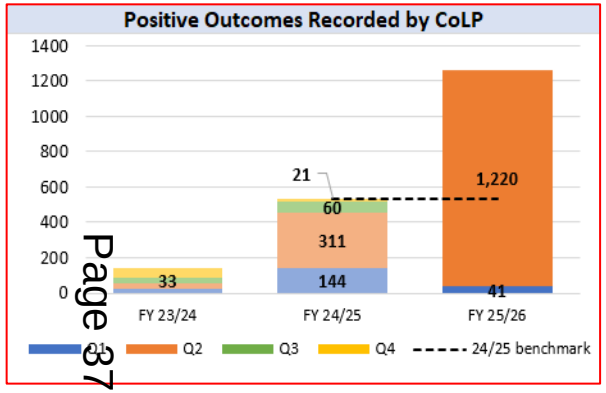
NLF also teamed up with The Traitors star Faraaz Noor to raise risk of Hajj related fraud, to which UK Muslims were being scammed when attempting to buy tickets to make the pilgrimage to Mecca.

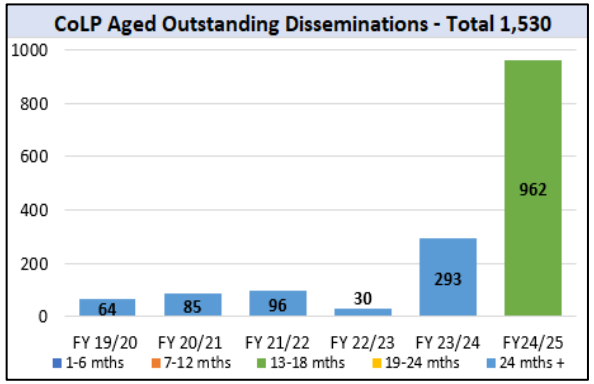
National Lead Force Fraud Operations: Includes National Fraud Squad Teams and Funded Units

Improve Outcomes for Victims

We will increase the policing response and outcomes linked to NFIB / Report Fraud crime dissemination packages. We will lead the National Fraud Squad to PURSUE identified high harm offenders through joint, centrally co-ordinated national operations and to participate in NECC led fraud intensifications throughout the year.

Success Measures:		
A. Increase the positive outcome rate for CoLP		
B. Decrease CoLP aged outstanding disseminations		
C. Support CoLP teams to engage in intensification efforts		





Positive Outcomes

- In Q4 CoLP teams recorded **14** positive outcomes and **1,464** no further action outcomes via the old outcome reporting methodology

It is not currently possible to establish total outcomes recorded in the quarter as the process for ensuring accurate recording and therefore reporting for both Pre and Post Report Fraud dissemination outcomes is still underway.

Outstanding Disseminations

- At the end of Q4, **1,530** disseminations from 19/20 to 24/25 were with CoLP teams awaiting outcomes
- This is **down 1% (-14)** for Q4 which is a reduction in outstanding outcomes, **this is positive**.
- It is not possible to include 25/26 disseminations in this measure yet.

Intensifications

Operation Henhouse was a fraud intensification coordinated by the NECC and CoLP, with intensified and coordinated PURSUE operational activity which took place throughout February. Data is still being collected and analysed by the NCA, however DCPCU have reported 31 arrests, £13,000 in cash seizures, £5,000 cryptocurrency seizures, £65,000 worth of listed assets, £10,000 value of ID printing equipment, £162,000 account freezing orders and £427,000 seized from a business account thought to be involved in money laundering.

Response

There are no upcoming intensifications or operations currently planned for Q1.

Response

Positive Outcomes

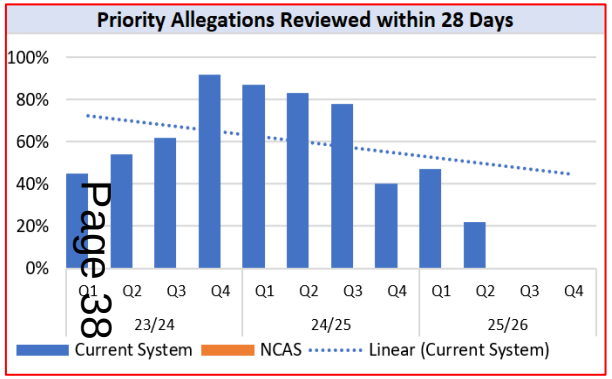
Work to identify recording of outcomes including refreshing the national guidance is underway and should allow for better reporting in future quarters for all outcome types.

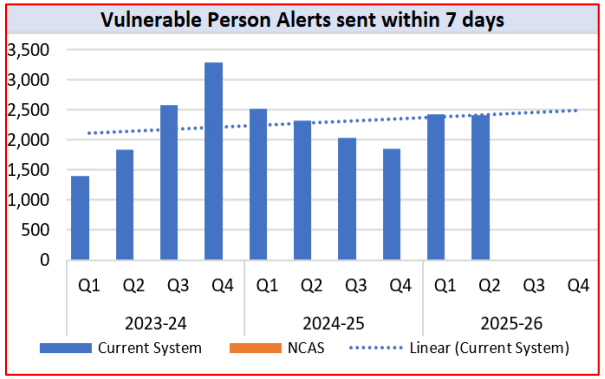
National Reporting Service: Includes Report Fraud Reporting Service, Analysis Service and Victim Services

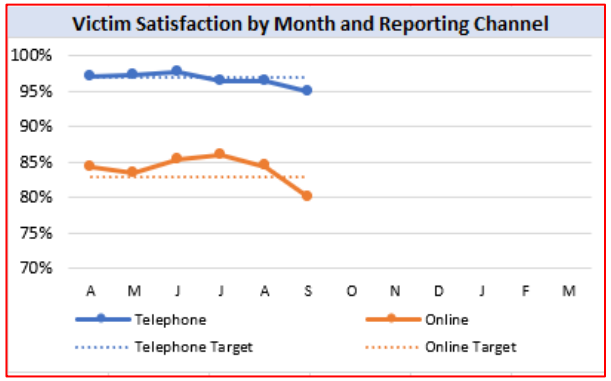
Proactively Pursue Offenders

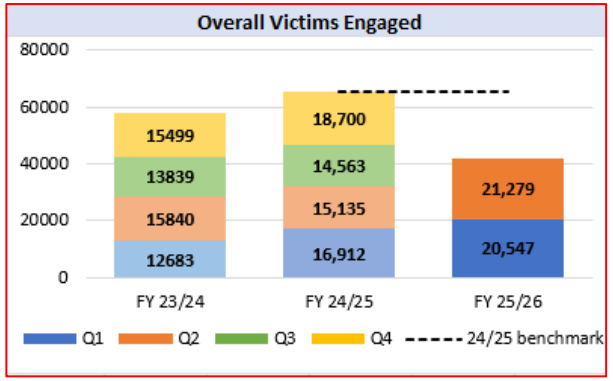
We will deliver the Fraud and Cyber Reporting and Analysis Service (FCCRAS) - including the ability to feedback intelligence into the system for further development and inclusion in intelligence packages. We will ensure intelligence is appropriately recorded and disseminated to assist with all 4P outcomes

Success Measures:		
A. Increase the allegations of fraud reviewed in 28 days meeting 'highly likely' & 'likely vulnerable' on the solvability matrix		
B. To review and, where appropriate, disseminate vulnerable person alert within 7 days		
C. Maintain the percentage of survey respondents who are satisfied with the Action Fraud reporting service		
D. Increase number of fraud victims who receive protect advice (NECVCU engagement)		









Report Fraud - Reporting, Analysis and Victim Services

The delivery of Report Fraud Reporting Analysis and Victim Services went live on 4th December 2025 with a public launch on 19th January 2026. The data platforms and reporting processes are still being refined, and it has not been possible to provide like for like information to be reported on for this performance product.

In the National performance report some information is provided about disseminations overall during the Q4 period.

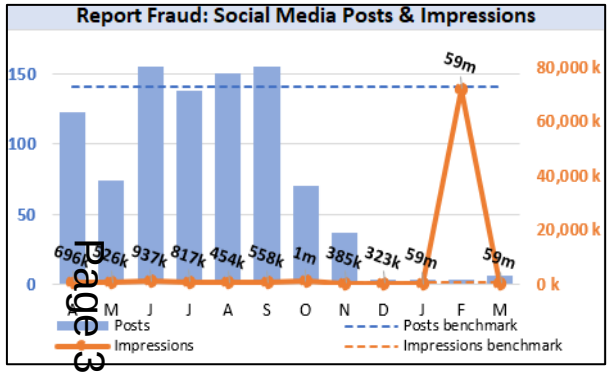
The Victim Satisfaction information is available within the new system however is not like for like the feedback has not significantly changed since Q3 in that people are positive about their initial experience with Report Fraud but are negative once an outcome is received.

National Reporting Service: Includes Report Fraud Reporting Service, Analysis Service and Victim Services

Improve Outcomes for Victims

We will improve the policing response to fraud.
Report Fraud objectives will be added when the system launches.

Success Measures:		
A. Increase the number of Report Fraud social media posts and impressions		⇨
B. Increase the number of P&D disruptions		⇧



Report Fraud Social Media

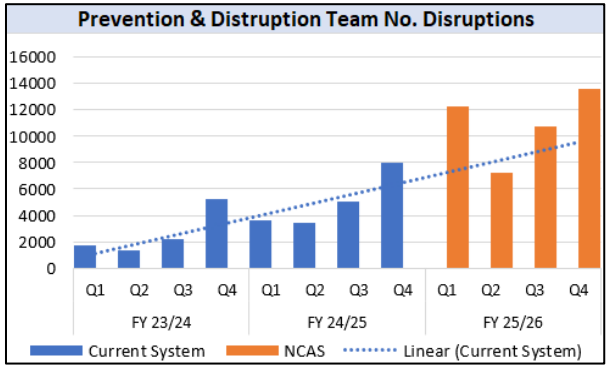
- Report Fraud made **12** posts in Q4, down **89% (-98)** from Q3.
- The related impressions for these posts totalled **72,202,592** an increase of **4,029% (+70,453,783)** from the previous year

Response

Report Fraud Social Media

In January 2026, the new national service for reporting cyber crime and fraud, Report Fraud, launch with an advertising campaign with earned and paid for social media.

The City of London Police worked with a marketing agency to produce a paid campaign for the launch, as well as the addition of earned media such as work with influencers and other media opportunities during this time – this explains the vast increase in impressions for Report Fraud social media channels in Q4.



Preventions and Disruptions

- In Q4 the P&D team carried out **13,531** disruptions, an increase of 26% compared to Q3 **(+2,764)**.
- Disruptions included:
- **1,407** website disruptions
- **1,372** email account suspensions
- **100** telephone deactivations
- **10,582** proactive domain suspensions
- **70** social media account suspensions

Growth is particularly evident with website disruptions and email account suspensions since the team started to use the National Crime Analysis System (NCAS).

Response

Prevention & Disruption

Increased performance by the Prevention and Disruptions team in Q4, particularly in Proactive Domain suspensions (Horizon Scanning / Nominet Alerts) is a result of Having significant success in identifying fraudulent, unlicensed gambling domains being registered and working with Nominet to have them suspended. Identifying individual personas registering malicious domains on mass, and targeting all domains registered to such individuals

In relation to reactive disruptions, particular success has been achieved in identifying and disrupting large volumes of malicious websites operating fraudulent "investment" scams.

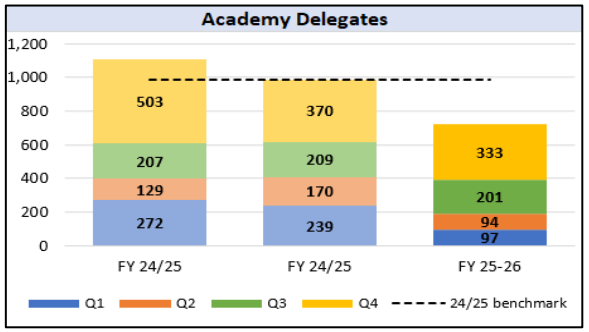
Economic Crime Police Headquarters: Includes Workforce Strategy, Economic Crime and Cyber Academy and Protect.

Protect People and Businesses

We will upskill and train our staff so that they are able to effectively respond to the threat of fraud, economic and cyber crime. We will roll out a revised performance framework across PURSUE, PROTECT, PREPARE and PREVENT. ROCUs and Forces to ensure completion of performance framework and resulting recommendations. We will invest in and explore technological and data sharing solutions and opportunities.

Success Measures:

A.	To increase delegate training levels in the Economic and Cyber Crime Academy (ECCA).		⇧
B.	Deliver objectives against National Workforce Strategy.		⇧
C.	Provide forces who are due to be inspected with specific pre-inspection support for delivering against the Fraud pillar within the PEEL framework		⇨



Academy

- In Q4 the ECCA held **28** courses, up **10% (+3)** from Q4 24/25
- At **333,** delegate numbers were down **10% (-37)** from Q4 24/25
- **94%** satisfaction was equal to Q4 24/25 and the benchmark

Response **Academy**

In Q4, the delivery of several Anti Money Laundering and Asset Recovery courses contributed to an increase in overall reach. A bespoke four-day training programme was also delivered in Bangkok, which received highly positive feedback from attendees.

Preparations has been made for the new financial year with the schedule of open courses planned, aligned to seasonal trends with bookings (e.g. a drop in Q1 as is seasonally seen).

Workforce Strategy

Highlights from prioritised workstreams under the National Policing People Strategy for Fraud, Economic and Cyber:

Direct Entry Detectives –progress on new pathway to recruit detectives who will focus on economic or cyber crime in partnership with Police Now. Cohort 1 - 12 CoLP officers started March 2025. 1 officer has resigned but all others are progressing and on their rotations. Cohort 2 - 8 CoLP officers started in March 2026. Cohort 3 - Planning underway with CoLP and partner forces (number TBC) to expand programme outside CoLP.

FIO Student Placements – Planning for expansion of scheme to further ROCUs and forces for Cohort 3 starting in Sept 2026.

Cohort 1 – 2 Students within CoLP in their part time year. Cohort 2 - 12 students on their placement years are now embedded within 4 ROCUs, MPS, and CoLP.

Volunteers – Funding agreed through the Cyber portfolio for two secondments to lead the national programme. Candidates have passed vetting and awaiting formal start dates.

Association of Economic Crime Professionals (AECP). CoLP working with the Home Office to deliver a united community of skilled professionals across the public and private sectors, to protect society from economic crime, enabling staff to enjoy rewarding, long-term careers in the field.

Complete workstreams include Career Pathways video for CoLP detailing key roles within Economic Crime, a Pay Parity Report, the inaugural Challenge Panel for practitioners on the Fraud Investigation Model, and the launch of the Living Library.

NCO - PEEL Support

The NCO are hosting two briefings in April with HMICFRS, Report Fraud Protect Team, ECPHQ and the Economic and Cyber Crime Academy to all forces.

This will pave the way to further host thematic workshops for attendance by all forces who have undertaken or are yet to undertake HMICFRS visits. Force visits are also predicted to continue as direct requests for support in anticipation of upcoming HMICFRS visits.

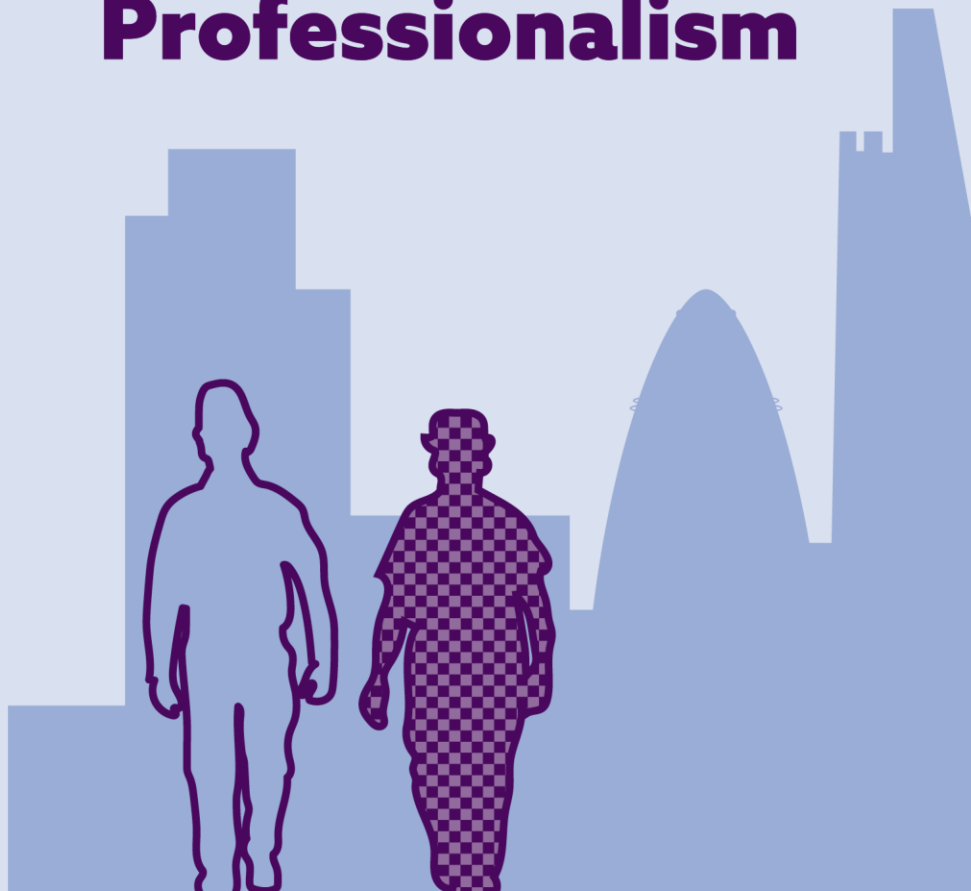
The NCO are not seeking to coach or mentor forces through those inspections but are providing forces with advice and guidance as to what good practice is when formulating a response to fraud.

Visits have declined for Q4 (5 visits) due to a reduction in staff alongside others waiting for the HMICFRS reports from force inspections.

Policing Plan Performance Fraud Slides Example

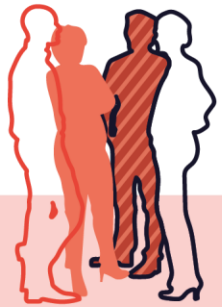
Quarter 1 2026/27

Integrity
Compassion
Professionalism



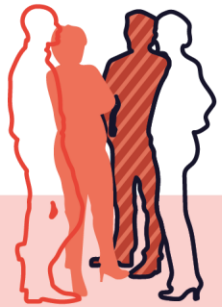
Performance Summary

Strategy Pillar	Performance Framework Headline Measure	Reporting Frequency	Latest Performance Assessment*	Data Maturity Assessment
Transform the national policing response to fraud, economic and cyber crime	Crime Reduction	Quarterly		
	Proactive Pursue	Quarterly		
	Stop & Block Protect	Quarterly		
	Traditional Protect	Quarterly		
	National Leadership Quality	Annually Q4		
Put victims at the heart of everything we do	Public Trust & Confidence	Quarterly		
	Reactive Pursue	Quarterly		
	Local Policing Response	Bi-annually (Q1 and Q3)		



Executive Summary

Transform the national policing response to fraud, economic and cyber crime	Put victims at the heart of everything we do



Transform the national policing response to fraud, economic and cyber crime

Crime Reduction

Quarterly performance RAG	Data trend
	⇨

Measure
At least a 10% reduction in average loss for Policing Control Strategy Fraud types – Abuse of Position, Courier Fraud, Romance Fraud (UK based), Investment Fraud.

Success measure reporting
Success will be measured by quarterly changes in the rolling 12-month median loss for each fraud type, with RAG ratings applied so that a quarterly success is recorded as green, modest improvement or minor increases are Amber, and significant increases are Red. A data trend will also be supplied looking for statistically significant changes across the data points.

How will this be reported
To report on this, we will use the loss figures for each of the control strategy fraud types from Report Fraud.

These will be combined to show the rolling 12-month median loss for the four control-strategy fraud types, updated quarterly to show whether victim harm is increasing or decreasing beyond normal tolerances.

Seasonal patterns will also be reviewed, and changes in median loss will be assessed alongside report volumes and losses per type to distinguish between genuine shifts in financial harm and fluctuations caused by increases or decreases in reporting as well the alignment to specific intensifications.

In response

Conclusions and recommendations will be added here to determine how performance can be improved in future quarters and what action is needed to improve or maintain in this area.

Proactive Pursue

Quarterly performance RAG	Data trend
	⇨

Measure
At least a 10% increase in total national value receipted from successful Asset Recovery proceedings.

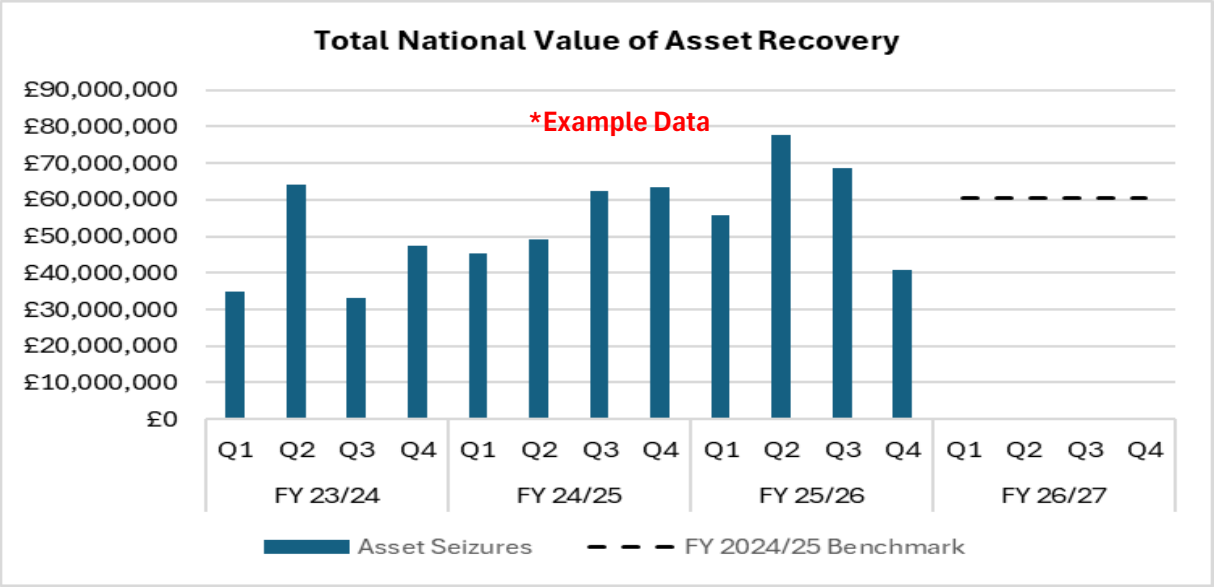
Success measure reporting
Success is evidenced on a quarterly basis by an increasing rolling 12-month total of national asset recovery, targeting ≥10% growth against the baseline for the last 3 years.

Green at ≥10% , Amber for modest gains, and Red for reductions.

A data trend will also be supplied looking for statistically significant changes across the data points to show long term trends.

How will this be reported
This will be based on the overall count of asset recovery compared to the average across the past 3 years (2023/4-2025/26) plus 10% from the NCA's published Joint Asset Recovery Data Dashboard.

This data set is subject to an approximate one-month lag this is due to the data being assured and cleansed by the team at the NCA. COLP cannot influence this lag and this may impact certain quarterly reporting where the timeframe between end of quarter and reporting are particularly small. Data for the latest period will be supplied and updated in the following quarter noting any differences made.



In response

Conclusions and recommendations will be added here to determine how performance can be improved in future quarters and what action is needed to improve or maintain in this area.

Stop and Block Cyber/Fraud Disruption

Quarterly performance RAG	Data trend
	⇨

Measure
At least a 1000% increase in the volume of instances where data sharing leads to offenders being stopped or blocked (ie removal of tech or finance identifiers enabling fraud, cyber and economic crime)

Success measure reporting
Success will be measured quarterly.

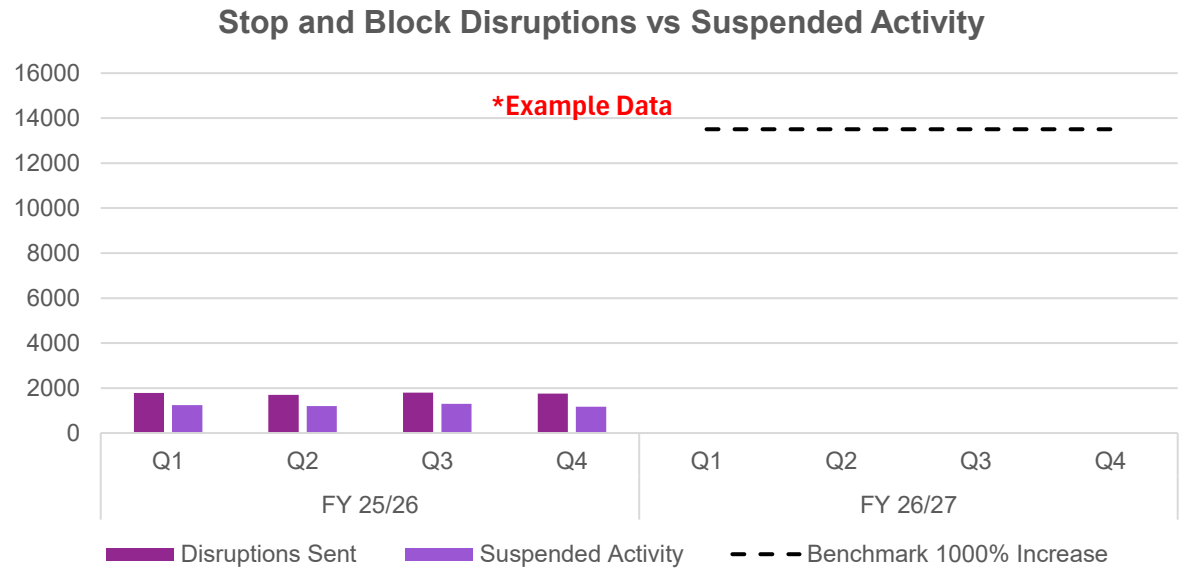
Confident data for confirmed removals is not available for past years this will need to be baselined in 2026/27.

As such in 26/27 the volume of referrals made will drive the quarterly performance and this will be compared against the service level for 27/28 once the baseline established. Work will continue to try and use alternative means to identify a baseline before April 2027 where possible.

A data trend will also be supplied looking for statistically significant changes across the data points to show long term trends.

How will this be reported
To report on this, we need to know the overall volume of disruptions sent to partners for removal, in addition to the total volume of confirmed takedowns from Report Fraud, such as confirmed removals of fraudulent websites, bank accounts, and other enablers, where police intelligence is sent to partners for action.

Data is still developing in Report Fraud and there may be a lag in the reporting of this by up to 1 month as the process develops. Data for the latest period will be supplied and updated in the following quarter noting any differences made.



In response

Conclusions and recommendations will be added here to determine how performance can be improved in future quarters and what action is needed to improve or maintain in this area.

‘Traditional’ Cyber/Fraud Protect

Quarterly performance RAG	Data trend
	⇨

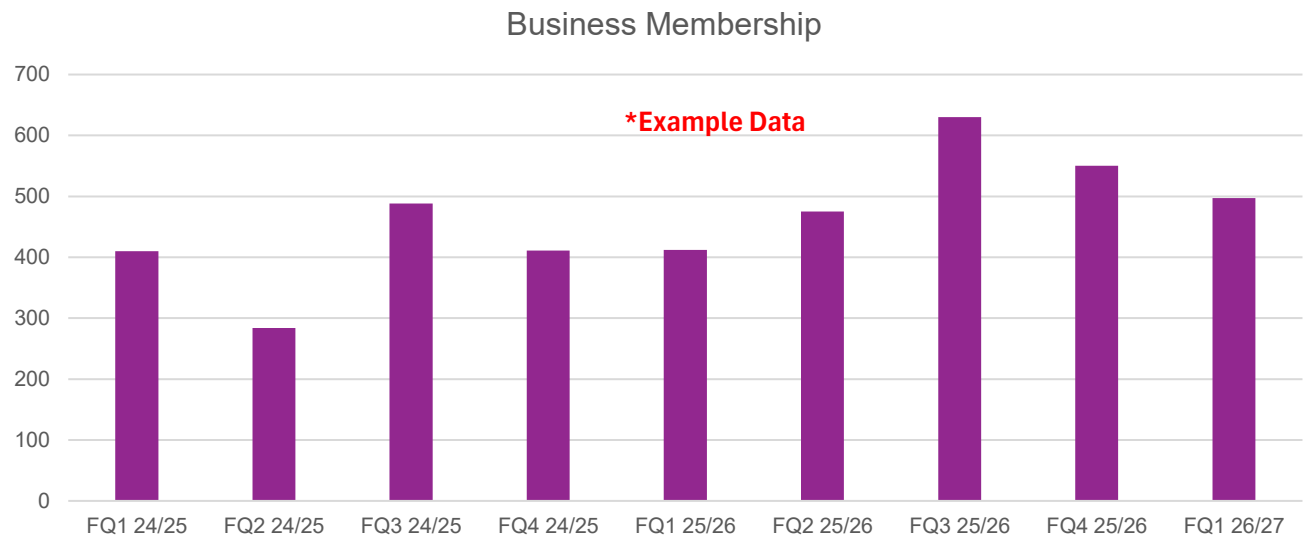
Measure
At least a 20% increase in the number of CRC businesses in membership

Success measure reporting
Success is evidenced on a quarterly, targeting ≥20% growth against the baseline for the last 3 years.

Green at ≥20% , Amber for modest gains, and Red for reductions.

A data trend will also be supplied looking for statistically significant changes across the data points to show long term trends.

How will this be reported
This is an overall count of active network memberships and is a cumulative total for active members at the end of each quarter; this is based on the original membership date in HubSpot. Which is facilitated by the CRC group.



In response

Conclusions and recommendations will be added here to determine how performance can be improved in future quarters and what action is needed to improve or maintain in this area.

‘Traditional’ Cyber/Fraud Protect

Quarterly performance RAG	Data trend
	⇨

Measure
At least a 500% increase in the national brand partnership reach figures.

Success measure and reporting methodology Success will be measured by quarterly changes in reach figures. It is still being established if there is an appropriate baseline for reach figures.

If one is not available 26/27 will be used to establish a baseline for increasing and performance will solely be reported on quarterly changes.

In response

Conclusions and recommendations will be added here to determine how performance can be improved in future quarters and what action is needed to improve or maintain in this area.

Put victims at the heart of everything we do

Public Trust and Confidence

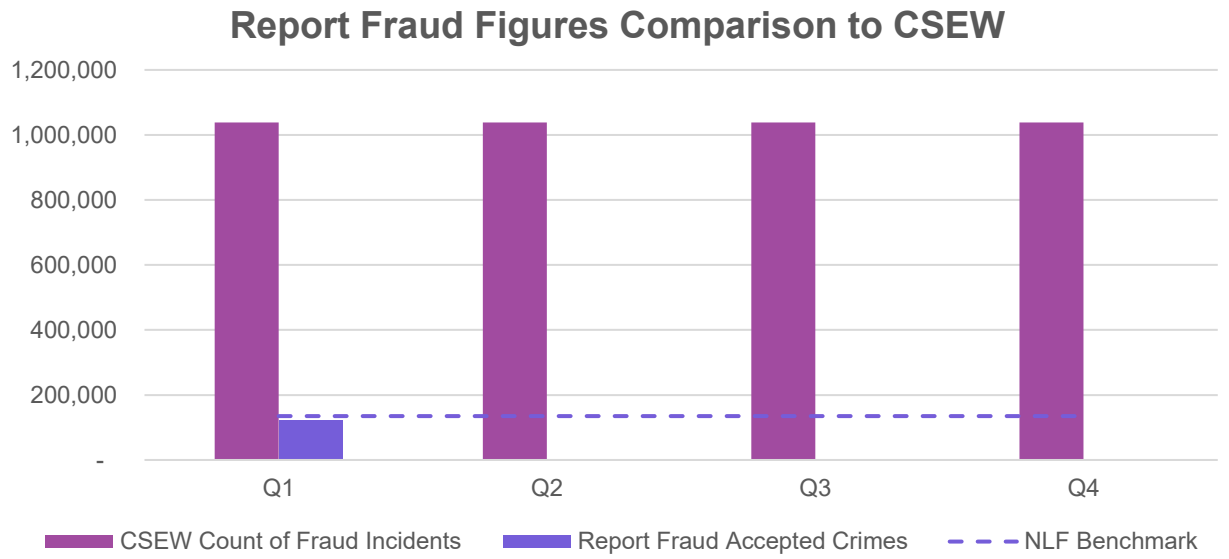
Quarterly performance RAG	Data trend
	⇨

Measure
A reduction in the gap between Report Fraud reports and CSEW estimates from 89% of crime estimated to be unreported, to 85%, across the 3year period.

Success measure reporting
Success will be measured by a 1% reduction in the under-reporting gap between CSEW-estimated fraud and police-recorded Report Fraud data each year, using the previous year as a baseline.

How will this be reported
To report on this, we need figures from CSEW on fraud level which are available publicly by the Office of National Statistics.
These will be compared against the total volume of accepted crimes into Report Fraud (irrespective of reporting method e.g. CIFAS, phone , online).
Each quarter, pair the latest ONS CSEW YE estimate with the matching rolling 12-month RF total then calculate the gap and the direction of travel toward 85%.

*Example Data



In response

Conclusions and recommendations will be added here to determine how performance can be improved in future quarters and what action is needed to improve or maintain in this area.

Reactive Pursue

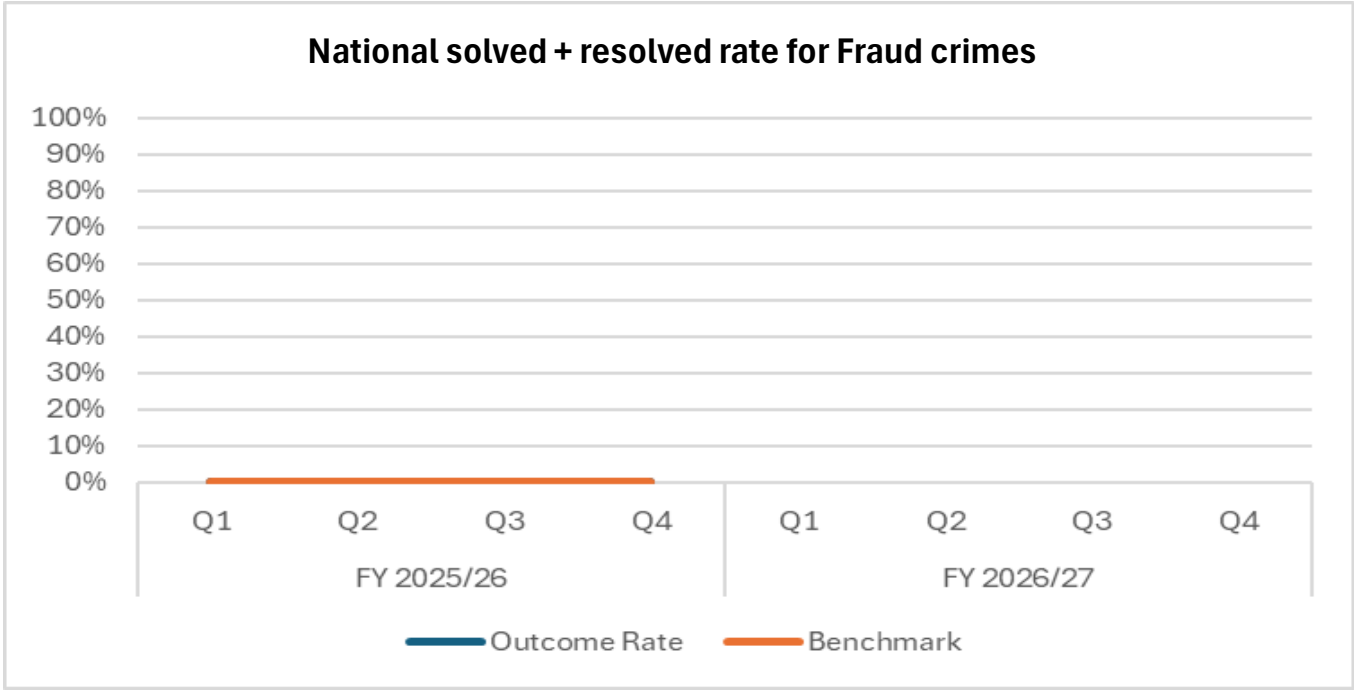
Quarterly performance RAG	Data trend
	⇨

Measure
Increase in Solved and resolved Outcome rate for all fraud crime reported to Report Fraud. At least a 5% increase across the 3 year period.

Success measure reporting
Success will be measured by a quarterly increase in the proportion of solved and resolved outcomes recorded in Report Fraud. As per the new outcome rate methodology identified by the Home Office for Crime reporting within the National Police Performance Framework.

How will this be reported
Data will be provided by Report Fraud for each quarter identifying the volume of outcomes overall and the breakdown across the categories of solved, resolved and unresolved thereby identifying outcome rate (this will be irrespective of when the crime was recorded or sent for investigation).

The change in that rate will be reported here including whether any changes are within normal tolerance levels or otherwise.



In response

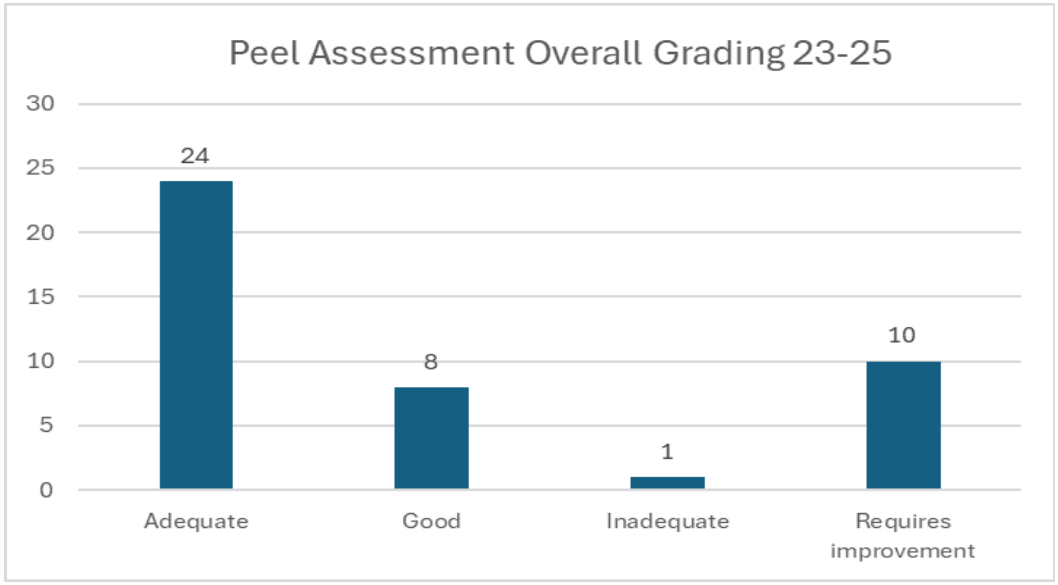
Conclusions and recommendations will be added here to determine how performance can be improved in future quarters and what action is needed to improve or maintain in this area.

Local performance in managing risk and serving the public

Measure
An increase in the proportion of forces achieve HMIC Outstanding, Good or Adequate (baseline from January 2026 when first moderated gradings will be released).

Success measure for reporting
Success will be measured by a bi-annually as report findings from PEEL are not released frequently.

How will this be reported
To evidence an increase in the proportion of forces achieving HMICFRS grades of Outstanding, Good or Adequate for fraud inspections, we need a centralised dataset that captures all moderated HMICFRS PEEL fraud gradings, beginning with the March release of the first tranche (following inspections conducted in June last year), which will form the baseline for the three-year performance period.
This will be collated through HMICFRS publications.



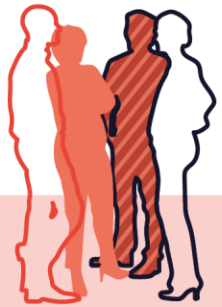
In response

Conclusions and recommendations will be added here to determine how performance can be improved in future quarters and what action is needed to improve or maintain in this area.

Appendices

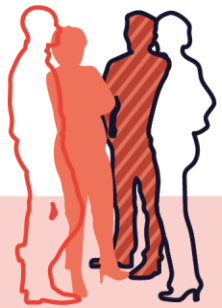
Data Maturity Assessment

Performance Framework Headline Measure	Data owner	Data Maturity Assessment	Data Maturity Narrative
Crime Reduction	COLP		
Proactive Pursue	NCA		
Stop & Block Protect	COLP		
Traditional Protect	COLP		
National Leadership Quality	TBC		
Public Trust & Confidence	COLP		
Reactive Pursue	COLP		
Local Policing Response	HMICFRS		

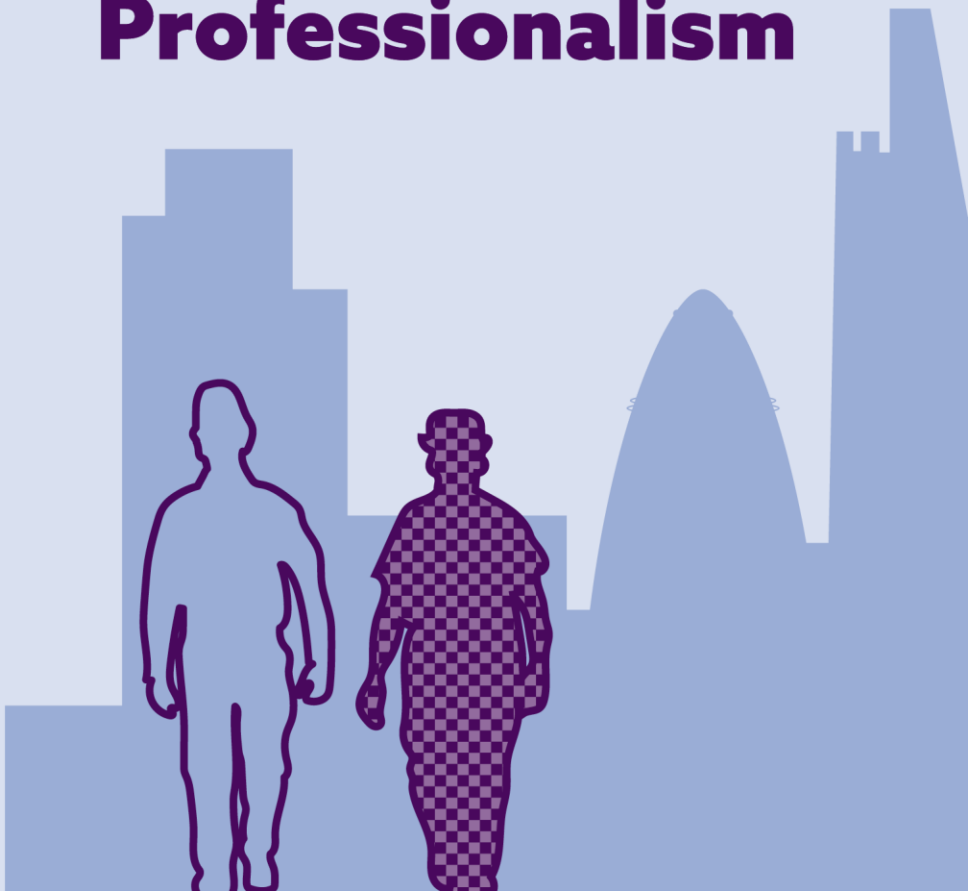


Success Measure Reporting

Performance Framework Headline Measure	Success measure reporting
Crime Reduction	
Proactive Pursue	
Stop & Block Protect	
Traditional Protect	
National Leadership Quality	
Public Trust & Confidence	
Reactive Pursue	
Local Policing Response	



Integrity
Compassion
Professionalism



This page is intentionally left blank

City of London Corporation Committee Report

Committee(s): Economic Security and Cyber Crime Committee (ESCCC)	**Dated:** 1st June 2026
Subject: Summary of Action Fraud public complaints data – Q4 2025/26	**Public report:** For Information
This proposal: • Provides statutory duties	Public trust and confidence
Does this proposal require extra revenue and/or capital spending?	No
If so, how much?	N/A
What is the source of Funding?	N/A
Has this Funding Source been agreed with the Chamberlain's Department?	N/A
Report of:	Commissioner of the City of London Police
Report author:	Detective Superintendent Tom Hill

Summary

The attached quarterly report produced by the Professional Standards Department provides members with an overview regarding Report Fraud complaints.

A total of 191 complaint cases were logged in Q4 2025/26. This is an overall increase 98 cases from Q3 2025/26 (+105%) Quarter 4 is above average with 114 cases logs on average over the previous 5 quarters is 114 per quarters.

Schedule 3 complaints increased from 1 to 5 in this quarter. Non-Schedule 3 complaints increased by 102% with the number of allegations also increasing significantly to 234 (+116%). This number is above the five-quarter average of 124.

The most common allegation category was "Police action following contact" (156), followed by "General level of service" (34) this was largely driven by unmet expectations regarding Report Fraud investigations. Reasons for complaint mostly

relate to customer expectations, with either the lack of contact or no investigation cited.

A backlog of complaints has developed over time, primarily due to a prolonged period of limited dedicated resource to manage non-Schedule 3 (S3) complaints for Action Fraud, with one full-time individual fulfilling this role. This has impacted timeliness in complaints handling; however, there has been a sustained focus on addressing this backlog, and performance has improved significantly. Timeliness for newly received complaints is increasing as a result.

Since the launch of the new system in December, there has been significant media attention, which has driven increased public awareness and a corresponding rise in the use of the Report Fraud service. PwC, as the third-party supplier for the contact centre, has reported consistently high volumes of calls and customer contact following the launch. As expected, increased demand has led to a higher volume of complaints, particularly as the system continues to embed.

Report Fraud remains in its early stages, and there is ongoing work to better understand the victim journey, respond to feedback, and implement improvements to processes. The end-to-end service is subject to continuous review to ensure it delivers the best possible experience for victims.

Professional Standards Department (PSD) and Report Fraud (RF) are working collaboratively, and the current resource model for complaint handling is under review to ensure it is resilient and capable of managing demand effectively. In parallel, workflows and processes are being refined to ensure they are proportionate to the nature of complaints and that handling is as efficient as possible.

Recommendation(s)

Members are asked to:

Note the report.

Appendices

- Appendix 1 – Summary of Report Fraud public complaints data– Q4 2025/26

Tom Hill
Detective Superintendent Tom Hill
Head of Professional Standards
T: 07803305003
E: thomas.hill@cityoflondon.police.uk

Summary of Report Fraud public complaints data– Q4 2025/26				
Metric	**Current quarter (Q4)**	**Previous quarter (Q3)**	**(%) change (Q on Q)**	**Comment**
Complaints – Schedule 3	**5**	**1**	**+400%**	A total of 191 cases were logged in Q4 2025/26. This is an overall increase of 98 cases from Q3 2025/26 (+105%) The average number of cases logged over the previous 5 quarters is 114 per quarter, Q4 is above average. AF changed to RF during Q3. This will be a period of change and PSD have amended the Centurion complaint database to reflect the name change. The IOPC have been made aware of the name change and have updated the bulletins accordingly.
Complaints – not Schedule 3	**186**	**92**	**+102%**	
Allegations	**234**	**108**	**+116%**	There were 234 allegations recorded in Q4 2025/26. This is an increase of 126 allegations from Q3 2025/26 (+116%). The average number of allegations over the previous 5 quarters is 124 per quarter. Q4 is above average.
Average time to log complaints (days)	**3**	**5**	**-40%**	*Timeliness is taken from IOPC published bulletins and available once published often retrospectively, unavailable dataset from Centurion.*
Average time to contact complainant (days)	**2**	**2**	**0**	
Complaints finalised – Schedule 3	**12**	**7**	**+53%**	A total of 65 cases were finalised in Q4 2025/26. This is an overall decrease of 26 cases from Q3 2025/26 (+29%) Average number of total cases finalised is 88 over the last 5 quarters. Q4 is therefore below average.
Complaints finalised - not Schedule 3	**53**	**84**	**-37%**	
Average time to finalise complaint cases (days) – Schedule 3	**217**	**243**	**-12%**	*Timeliness is taken from IOPC published bulletins and available once published often retrospectively.* *IOPC bulletins published breakdown by case type logged (Q4 provides the full yearly data)*
Average time to finalise complaint cases (days) – not Schedule 3	**198**	**185**	**+7%**	
Applications for review sent to local policing body	**5**	**0**	**0**	5 non-investigation reviews recorded during Q4.

Applications for review sent to IOPC	**0**	**0**	**0**	None recorded during Q4

Nature of allegations – Of the 234 allegations recorded during Q4 2025/26 the highest number was in the category of, A1 – Police action following contact (156) followed by General level of Service (34) Reasons for complaint mostly relate to customer expectation of Report Fraud, with either the lack of contact or investigation cited. This is an increase in allegations recorded against Q3 of 126 (116%).

Members of Parliament –

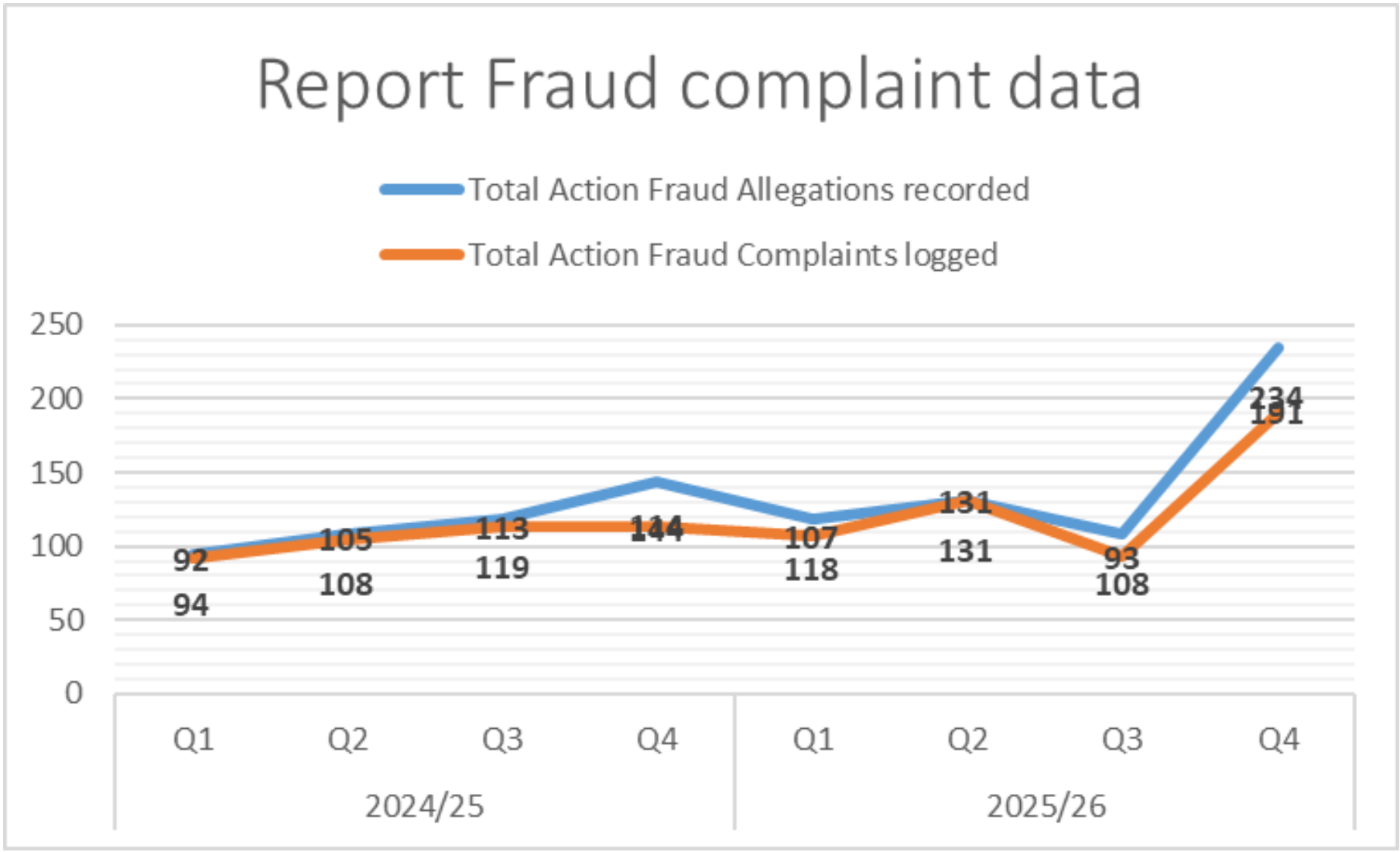
There have been 87 miscellaneous cases logged where MPs have made contacted to CoLP on behalf of a constituent. This is an increase of 51 against the previous quarter. The average being logged as 71 over the last 5 quarters.

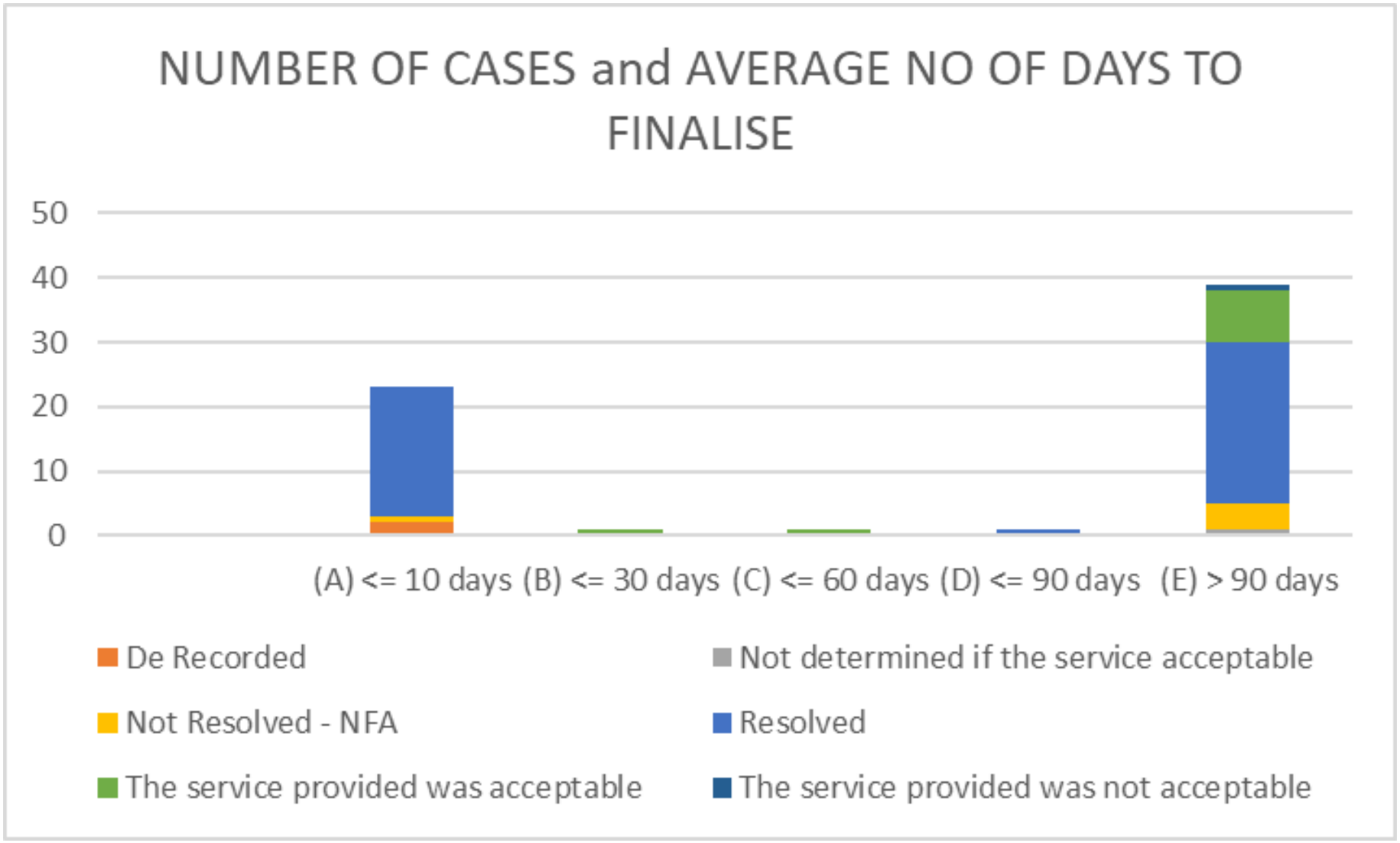
Report Fraud Complaint Recording –

The Report fraud (RF) system 'switch over' from Action Fraud (AF) occurred during Dec 2025. There is likely higher recording of fraud on the new RF system due to the improvements made to the service, which has greater accessibility, and automation to the reporting service.

There is an upward trend on the use of Large Language Models such as ChatGPT and A.I in the assistance to compose complaints. By complainants using A.I there is an increase in the requirement to record under Schedule 3, for investigation assessment, and potential review.

Report Fraud complaints are recorded in Professional Standards (PSD). National Lead Force (NLF) review the complaint (as subject matter experts). During 2025-26 a total number of 254 (outside Schedule 3) complaints were recorded that took an average of 198 days to finalise. 44 complaints (schedule 3) were recorded and took an average of 217 days to finalise. PSD are now recording complaints of complainants who have not had a response to their original complaint from NLF.


Report Fraud complaint data
Total Action Fraud Allegations recorded
Total Action Fraud Complaints logged
250
200
150
100
50
0
92
94
105
108
113
119
144
107
118
131
131
93
108
234
191
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
2024/25
2025/26


NUMBER OF CASES and AVERAGE NO OF DAYS TO FINALISE
50
40
30
20
10
0
(A) <= 10 days
(B) <= 30 days
(C) <= 60 days
(D) <= 90 days
(E) > 90 days
De Recorded
Not determined if the service acceptable
Not Resolved - NFA
Resolved
The service provided was acceptable
The service provided was not acceptable

Committee(s): Economic Security & Cyber Crime Committee	**Dated:** 23/06/2026
Subject: Innovation & Growth – Update on Economic Security and Cyber Crime related activities	**Public report:** For Information
This proposal: • **delivers Corporate Plan 2024-29 outcomes** • **provides statutory duties** • **provides business enabling functions**	Dynamic Economic Growth
Does this proposal require extra revenue and/or capital spending?	No
If so, how much?	N/A
What is the source of Funding?	N/A
Has this Funding Source been agreed with the Chamberlain's Department?	N/A
Report of: Executive Director, Innovation and Growth	Damian Nussbaum
Report author: Head of FPS Technology, Innovation & Growth	Melissa Panszi/Mary Kyle

Summary

The core objective of Innovation & Growth (IG) is to strengthen the UK's competitiveness as the world's leading global hub for financial and professional services (FPS). This includes promoting the strengths of the UK's offer and enhancing the UK's position as a leader in FPS technology and innovation.

As the national lead force for fraud and NPCC lead for cyber, the City of London Police (CoLP) plays an important role in helping to build a resilient and secure eco-system in which both individuals and businesses across the UK can operate safely. The work of Innovation & Growth (IG) and CoLP therefore remains closely aligned.

The following report summarises the activity that has been taking place across IG in relation to cyber and economic crime since the Economic Security and Cyber Crime Committee last convened in February 2026.

Links to the Corporate Plan

1. The activities set out in this report help deliver against the Corporate Plan's aim to support a thriving economy. This includes outcome 6c - to lead nationally and advise internationally on the fight against economic and cybercrime. It also supports outcome 7, positioning the UK as a global hub for innovation in financial and professional services.

Main Report

Innovation & Growth/City of London Police cross-team working

2. We continue to use this report to review those activities which demonstrate the benefits of IG and CoLP collaboration. IG continues to look for ways to promote the activity of CoLP and support their work as part of our wider stakeholder engagement.

Collaboration

Financial Action Task Force (FATF)

3. As a result of the collaboration between the PAB and IG to engage with HMT on the forthcoming Financial Action Task Force (FATF) evaluation of the UK's anti-money laundering regime, the City hosted FATF's Learning and Development Forum, a meeting of supervisors that supports the implementation of FATF's risk-based approach to standards. The forum took place on 25–26 February at the Barbican, and a reception (sponsored by the Police Authority) was hosted at Mansion House.

4. The event marked a significant milestone in advancing shared priorities on improving the effectiveness of the risk-based approach, creating space for practical discussion between international counterparts and industry, and helping to challenge and strengthen supervisory and enforcement approaches. It also showcased London and the UK at our best: a global centre for financial and professional services, and a jurisdiction committed to strong collaboration and innovation in tackling economic crime.

Police Reform

5. IG has been supporting the CoLP through the police reform process over the last couple of months.

Embedded support and senior engagement

6. IG has been embedded across key governance and delivery forums (including Operation North Star, Reform Programme Board, and business engagement groups), ensuring consistent, hands-on support. With a particular focus on business engagement in support of CoLP's role, and input on the importance of the City's role in the UK economy.

7. Alongside this, IG has maintained close engagement with senior CoLP and CoLC leadership, enabling ongoing strategic advice, alignment with City priorities, and effective cross-Corporation coordination.

Strategic advice and policy development

8. IG has played an active role in helping shape, draft and strengthen key reform proposals: the Police Reform Response, National Lead Force proposal, and 1 Salisbury Square development.

9. This has included strengthening narrative, particularly the unique role of the City of London as a global financial centre and its importance to the UK's economic growth. And supporting the delineation of the future role of the police as National Lead Force. This has helped ensure that proposals are robust, clearly positioned, and aligned - strengthening narrative, structure and the case to both government and industry.

Business engagement and communications

10. IG has worked closely on business engagement over the past 12 months with activity intensifying in recent months. The past month IG has co-led the development of a coordinated, targeted business engagement approach—identifying and prioritising key FPS stakeholders, supporting senior outreach, and ensuring consistent messaging.

11. This has encompassed a structured identification and prioritisation exercise of key FPS stakeholders to focus engagement on the most influential voices and secure targeted support. IG has also facilitated direct dialogue between CoLP leadership and senior FPS stakeholders through a series of set-piece dinners and events, providing structured opportunities for principal-level engagement.

12. Alongside this, IG has helped develop effective and consistent messaging. To strengthen positioning and stakeholder engagement. This has spanned: drafting tailored and personalised communication for priority stakeholders; input into briefing materials and the core value proposition; and the development of wider core messaging. This has helped ensure a more consistent and impactful external narrative.

Delivery discipline and coordination

13. IG has supported the introduction of greater structure to engagement through centralised tracking and reporting, improving coordination, accountability and visibility. With the development of a centralised feedback and reporting mechanism. Specific outputs include sitreps, business engagement process updates, deployment cycle from conception to delivery and presenting options via the governance structure.

.

Innovation & Growth activity

<u>RegTech</u>

14. Regulatory Technology (RegTech) focuses on developing technological solutions that enable regulated firms to meet compliance and regulatory requirements more efficiently and effectively. Last year the City of London Corporation (CoLC) and Innovate Finance launched the RegTech Strategy Group to position RegTech as a

major UK export sector, contribute to the Government's wider growth agenda, expand the UK RegTech sector by 20%, and significantly reduce compliance costs over the next five years.

15. Building on the outputs from the first three meetings between October and March 2026, the RegTech Strategy Group will now move into a delivery phase focused on three priority themes (data access, digital verification, investment and skills). These themes will be developed by three working groups to deepen analysis of the key barriers to RegTech adoption and to develop practical, actionable recommendations.

16. The working groups will be delivered through a series of targeted workshops, with one to two sessions planned for each topic between June and July. These sessions will bring together relevant industry, regulatory and academic expertise to refine the problem statements, test potential solutions, and identify priority areas for action.

17. Outputs from the workshops will feed into a consolidated, overarching report planned for publication in October, which will set out recommendations for industry and policymakers, and identify areas for future collaboration.

Digital Verification

18. The City of London Corporation's Securing growth: the digital verification opportunity report (March 2025) articulated the need for UK-wide digital verification service (DVS) to combat fraud of and introduce efficiencies into our financial system around the sharing of personal and organisational data. Such a system needs an underlining operating platform on which personal data, organisational data and other information can be shared safely and speedily, a digital verification orchestrator.

19. The City of London established in February 2026, the Digital Verification Orchestrator Initiative (DVO), with the aim of establishing a trusted, interoperable framework for digital identity verification in the UK.

20. The DVO Initiative is chaired by Ezechi Britton MBE, with Sushil Saluja CC, Innovation and Tech Lead at the City of London Corporation, as Vice Chair. The Initiative is supported by the DVO Initiative Working Group and Steering Committee (SteerCo). Membership includes some of the UK's largest banks and FinTechs, representatives from academia, trade associations and institutes, as well as representatives from legal firms and consultancies.

21. On the 30th of June, the initiative will be launching a DVO blueprint, which will outline the governance structure, commercial model, liability allocation, technical and security standards, and participation rules for a DVO. The blueprint will also identify existing market capabilities and will set out recommendations to continue scaling the DVO model. The blueprint will serve as a guide for industry, regulators and potential DVO candidates to align on a neutral, scalable and legally robust DV ecosystem. This work supports the City Corporation's Vision for Economic Growth recommendation to scale digital verification across UK financial services.

Department for Business and Trade: Call for input on Powers to protect the UK from adverse economic pressure

22. The City of London Corporation participated in a roundtable on the 18th of May organised by the Department for Business and Trade to discuss proposed powers to protect the UK from adverse economic pressure. Industry participants raised the following concerns:

    - Risk of increased regulatory complexity and market impact, undermining the UK's reputation as a predictable, open market.
    - Implementation challenges, including setting the appropriate threshold, managing interactions with international frameworks, and applicability within services markets.
    - Preference for a diplomacy-led approach, given the risk that even signalling measures about the introduction of these powers could trigger destabilising relation dynamics.

    The Corporation will submit a formal response to this consultation, which closes on the 18th of June.

23. Strategic implications - This work supports the Corporate Plan outcome to drive dynamic economic growth.

24. Financial implications - All budgets are contained within existing departmental budgets and business planning.

25. Resource implications - All resourcing requirements are scoped as part of departmental business planning.

26. Legal implications - None identified for this paper.

27. Risk implications - None identified for this paper.

28. Equalities implications - The stakeholder work as part of this work is mindful of balancing the needs to have the right stakeholders identified while also supporting the CoLC's EDI commitments.

29. Climate implications - None identified for this paper.

30. Security implications - None identified for this paper.

Conclusion

IG will continue to engage with the CoLP and the PA on economic crime and cyber through the ongoing initiatives set out in this paper, particularly throughout the process of making the City's case to Government about the future of the City of London Police, as well as any emerging issues that may arise.

Melissa Panszi/Mary Kyle
Head of FPS Technology
E: Melissa.Panszi@cityoflondon.gov.uk/Mary.Kyle@cityoflondon.gov.uk

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank